

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43084 A2

(51) International Patent Classification⁷: **G07F**
(21) International Application Number: PCT/US00/42592
(22) International Filing Date: 5 December 2000 (05.12.2000)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
09/455,289 6 December 1999 (06.12.1999) US
(71) Applicants and
(72) Inventors: **PIELEMIEIER, Ted, A.** [US/US]; Suite 125,
13907 Montfort Drive, Dallas, TX 75240 (US). **STEIN-
BERGER, Lance, T.** [US/US]; 125 Baird Circle, Highland
Village, TX 75077 (US). **PHILIP, Rolfe, M.** [CA/US]; 130
Rassani Drive, Danville, CA 94506 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK,
DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,
LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT,
RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA,
UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,
CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

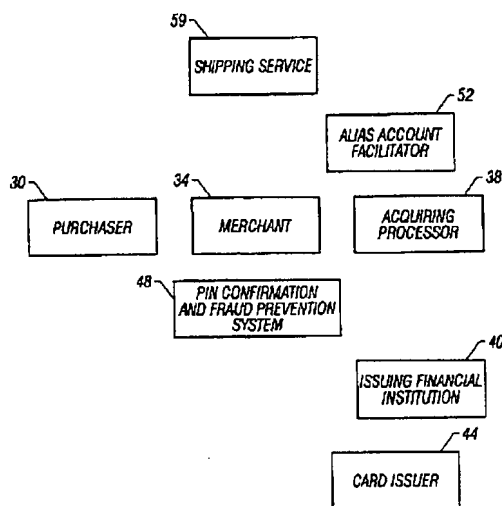
Published:

— Without international search report and to be republished
upon receipt of that report.

(74) Agent: **SMITH, Steven, W.**; Smith, Danamraj & Youst,
P.C., Suite 1200, LB-15, 12900 Preston Road, Dallas, TX
75230-1328 (US).

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF MASKING THE IDENTITY OF A PURCHASER DURING A CREDIT TRANSACTION



(57) Abstract: A method of masking the identity of a purchaser (30) during a credit transaction. The method includes the steps of establishing an alias credit account associated with the purchaser. The alias credit account includes an alias name and alias account number. The purchaser buys a selected item by utilizing the alias credit account. The alias account is then verified as a valid account having adequate credit to purchase the selected item. Next, the alias account is associated with the purchaser. The selected item may then be delivered to an alias address allowing pickup of the selected item by the purchaser or to his home address without the merchant knowing the purchaser's home address or the shipper knowing the nature of the item.

WO 01/43084 A2

METHOD OF MASKING THE IDENTITY OF A PURCHASER DURING A CREDIT TRANSACTION

5 TECHNICAL FIELD

This invention relates to credit transactions, and more particularly, to a method of masking the identity of a purchaser during a credit transaction.

BACKGROUND ART

10 The use of credit cards has increased tremendously over the last few years. However, the popularity of credit cards has not completely translated to the Internet. Recent polls indicate that most people are reluctant to purchase anything via the Internet due to concerns over lack of privacy when using a credit card through the Internet. There are several problems associated with the use of a credit card, whether over the Internet, a telephone, via mail, or
15 even in person. During a credit card transaction, several parties (e.g., the merchant, a credit card issuer, and various financial institutions) may know the name, credit card number, billing address, and shipping address of a buyer. The merchant is also able to collect a detailed list of the items the buyer has purchased. It is a common practice for the merchants, credit card issuers, and financial institutions to sell this information to marketing firms. This information
20 may be linked to other databases to form vast databases detailing personal information on a large amount of people. This collection and transfer of information results in a large amount of unwanted solicitations, such as junk mail and telephone solicitations.

Identity theft is another serious problem resulting from using a credit card, especially over the Internet. Identity theft accounts for over \$100 million lost each year. Studies also
25 indicate that the crime of identity theft is on the rise. Identity theft occurs when a thief obtains the credit card number and name of an individual. With this information, the thief can request and receive other credit cards and other forms of identification associated with the individual. In essence, the thief "steals" the identity of the individual. The theft of the individual's identity can result in ruined credit, bill collector harassment, criminal records and mixed up
30 identities for the innocent credit card user.

Lack of privacy is perceived to be especially acute by the consumer when using a credit card over the Internet. Therefore, many consumers are reluctant to purchase items over

the Internet, resulting in billions of dollars of lost sales. Improved privacy is necessary to increase credit card sales, especially over the Internet.

Although there are no known prior art teachings of a solution to the aforementioned deficiency and shortcoming such as that disclosed herein, prior art references that discuss subject matter that bears some relation to matters discussed herein are U.S. Patent Number 4,055,746 to Peterson (Peterson), U.S. Patent Number 5,224,162 to Okamoto et al. (Okamoto), U.S. Patent Number 5,420,926 to Low et al. (Low), and U.S. Patent Number 5,889,862 to Ohta et al. (Ohta).

Peterson discloses a method of securely using a credit card by utilizing a card having a plurality of ferromagnetic elements, capable of storing binary indicia, sandwiched between thin sheets of a non-magnetic material. Adopted names are provided on two faces and four edges of the card to provide security. The card may be inserted into a computer in any one of eight ways. When the proper adopted name is selected, the stored information on the card is released. The card owner knows the adopted name while an imposter has only one chance in eight of properly inserting and using the card. However, Peterson does not teach or suggest a parallel anonymous credit card account associated with an existing credit card account. Additionally, Peterson does not solve the privacy problems associated with credit card transactions. Peterson also suffers from the disadvantage of requiring a complex new type of credit card for use in transactions.

Okamoto discloses an electronic cash system utilizing a blind signature system in which a user has electronic cash and a license issued by a bank showing that the user is entitled to use the electronic cash. The user presents to a store the electronic cash, information containing the license, and a composite number which is the product of at least two prime numbers. The store checks the validity of the license and the composite number, and if they are valid, prepares and offers an inquiry to the user. In reply to the inquiry, the user computes a power residue of a desired function using the composite number as a modulus and shows it as a response to the store. The store then verifies the validity of the response through the utility of the composite number, and, if valid, acknowledges the payment with electronic cash of the amount of money to be used. However, Okamoto does not teach or suggest a parallel anonymous credit card system. Okamoto merely discloses utilizing a complicated blind signature system which requires complex calculations by both the card user and the bank during any transaction.

Low discloses a method of performing credit card transactions without disclosing the subject matter of the transaction to the institution providing the credit card. The method includes the use of a communications exchange so that information and funds may be transferred without the destination for the transfer knowing the source of the information or funds and the use of public key encryption so that each party to the transaction and the communications exchange can read only the information the party or the exchange needs for its role in the transaction. However, Low does not teach or suggest associating an anonymous credit card account with an existing credit card account. Additionally, Low suffers from the disadvantage of requiring two banks to implement and use the system, resulting in higher transaction costs.

Ohta discloses a method of implementing traceable electronic cash. A user sends both public and secret information with his real name to a bank. The bank recognizes the user's identity and generates a pseudonym of the user. The bank uses a signature function to attach a signature to information composed of the public information and sends the user the signed information with a license. The user generates authentication information and sends the authentication to the bank, using a blind signature system. If the user abuses the electronic cash, the bank files a court order to reveal the correspondence between the real name and pseudonym of the user and trace the electronic cash spent. However, Ohta does not teach or suggest implementing a parallel anonymous credit card account associated with an existing accounting. Ohta also requires utilizing a blind signature scheme which is complex and expensive to implement.

Review of each of the foregoing references reveals no disclosure or suggestion of a method as that described and claimed herein. Thus, it would be a distinct advantage to have a method which provides a simple and inexpensive way of masking the identity of a credit user during a credit transaction. It is an object of the present invention to provide such a method.

DISCLOSURE OF INVENTION

In one aspect, the present invention is a method of masking a true identity of a purchaser during a credit transaction. The method begins by establishing an alias credit account associated with the purchaser. The alias credit account masks the true identity of the purchaser by displaying only alias information. Next, the purchaser conducts a credit transaction by

buying a selected item using the alias credit account. The alias credit account is then associated with the purchaser.

In another aspect, the present invention is a method of conducting an anonymous credit card transaction by a purchaser. The method begins by the purchaser ordering a selected item.

5 The purchaser utilizes an alias credit account having alias information of the purchaser. The alias credit account is associated with a core account having a real identity of the purchaser. Next, a credit transaction for the selected item is authorized, and the selected item is then sent to the purchaser.

In still another aspect, the present invention is a method of masking a true identity of
10 a purchaser during a credit transaction. The method starts by establishing an alias credit account associated with the purchaser. The alias credit account includes an alias name masking the true identity of the purchaser and may also include an alias account number, an alias address, and an alias Personal Identification Number (PIN). The purchaser then conducts a credit card transaction to purchase a selected item using the alias credit account. The alias
15 account is then verified as a valid credit account, and it is verified that sufficient credit is available to purchase the selected item. The alias credit account is associated with a core account displaying the true identity of the purchaser. The core account is then debited for the credit card transaction.

In another aspect, the present invention is a method of masking a true identity of an
20 individual requiring a credit status report to complete a transaction. The method begins by the individual establishing an alias account. Next, the individual conducts the transaction requiring a credit status report using the alias account. The financial institution then requests the credit status report. The alias account is associated with the individual. Next, the credit status report is sent to the financial institution.

25 In another aspect, the present invention is a method of masking a true identity of an individual during a transfer of medical records of the individual from a first health care provider to a second health care provider. The method begins by transferring the medical records to a service organization. Next, the true identity of the individual is masked on the medical records by the service organization. The service organization then transfers the
30 masked medical records to the second health care provider.

BRIEF DESCRIPTION OF DRAWINGS

The invention will be better understood and its numerous objects and advantages will become more apparent to those skilled in the art by reference to the following drawings, in conjunction with the accompanying specification, in which:

5 FIG. 1 (Prior art) is a block diagram illustrating existing credit card transactions;
 FIG. 2 is a block diagram illustrating a credit card transaction of a purchaser utilizing an alias account in accordance with the teachings of the present invention;

 FIGs. 3A and 3B are flow charts outlining the steps for processing a credit card transaction utilizing an alias account in the preferred embodiment of the present invention;

10 FIGs. 4A and 4B are flow charts outlining the steps for processing an alias credit card transaction through the alias account facilitator in an alternate embodiment of the present invention;

 FIGs. 5A and 5B are flow charts outlining the steps for processing a alias credit card transaction through the alias account facilitator 52 acting as an Independent Service
15 Organization (ISO) in an alternate embodiment of the present invention;

 FIGs. 6A and 6B are flow charts outlining the steps for establishing an alias account by the purchaser having an existing account in the preferred embodiment of the present invention;

 FIGs. 7A, 7B, and 7C are flow charts outlining the steps for establishing an alias
20 account by the purchaser requiring a primary core account in the preferred embodiment of the present invention;

 FIG. 8 is a top level block diagram illustrating a system configuration of an alias account system in the preferred embodiment of the present invention;

 FIG. 9 is a diagram of high level information transfer by the alias account system in
25 the preferred embodiment of the present invention;

 FIG. 10 is a block diagram illustrating a medical transaction of a purchaser utilizing an alias account in accordance with the teachings of the present invention; and

 FIG. 11 is a block diagram illustrating a transaction for determining a credit status of a customer utilizing an alias account in accordance with the teachings of the present invention.

30

MODES FOR CARRYING OUT THE INVENTION

A method of masking an identity of a person during a transaction is disclosed.

FIG. 1 is a block diagram illustrating an existing credit card transaction. A purchaser 10 buys an item from a merchant 12 using a credit card. The merchant requests authorization for the credit card transaction by communicating with an authorization center 14 via a communications link 16. In most cases, the link 16 is a direct electronic link to the authorization center. The authorization center then verifies that the purchaser's credit card account is a valid account and has available credit by querying an issuing financial institution/card issuer 18 via a communications link 20. The issuing financial institution/card issuer keeps and processes all transactions of the purchaser's credit card account. The issuing financial institution/card issuer then responds to the query by either authorizing or rejecting the requested credit card transaction. The authorization center then relays the authorization or rejection message to the merchant. The merchant, upon receiving proper authorization from the authorization center, delivers the item to the purchaser.

Several problems arise from existing credit card transactions. Various financial institutions/card issuers and merchants keep large databases storing the credit card transactions of their customers (purchaser 10) and other account information, such as the home address, telephone number, and other personal data of their customers. Typically, these financial institutions sell this information to various marketers, thereby violating the privacy of the purchaser. This may result in the purchaser receiving numerous solicitations, such as mailings and telephone calls.

Other problems also result from utilizing the existing credit card system. At times, the name and credit card number are obtained by thieves during the transaction process. The thieves use this information to establish new credit card accounts, and are actually stealing the "identity" of the purchaser. This information may be stolen from various sources during Internet purchases, telephone purchases, live purchases, discarded credit card receipts and statements, and other sources.

In existing credit card systems, a single account is utilized. The account usually includes personal information necessary to process any credit card transaction. Personal information may include account name, account number, billing address, telephone number, and password identifier (for example, the maiden name of the purchaser's mother), as well as other personal information data necessary to initially establish the account.

In the preferred embodiment of the present invention, a separate parallel "alias" account is established and associated with the primary "core" account. In other embodiments, the parallel alias account may also be used by multiple core accounts. Additionally, multiple alias accounts can be set up and used for a single core account (e.g., family members each having individual accounts linked to a single core account). The parallel alias account may include an alias account name, alias account number, an alias address, and a password identifier (e.g., mother's maiden name). The alias account is used by a purchaser to mask the true identity of the purchaser when privacy regarding the purchaser's credit card transactions is desired. In addition, a second alias account may be established utilizing a back-up alias account name, a second alias account number, a second alias address, and a password identifier. The back-up alias account may be used when the first alias account(s) is compromised. The purchaser may also have a plurality of back-up accounts.

FIG. 2 is a block diagram illustrating a credit card transaction of a purchaser 30 utilizing an alias account accordance with the teachings of the present invention. In the preferred embodiment of the present invention, the purchaser communicates through a data network, such as the Internet. In alternate embodiments, the purchaser communicates via telephone, mail, or in person to a merchant 34. The merchant 34 may have a web site accessible through the Internet, a telephone receiving system, or a mail order address. The merchant communicates with an acquiring credit card processor 38, which typically processes credit card transactions utilizing the Automated Clearing House (ACH) Network to authorize a credit card transaction. The ACH Network is a processing and delivery system that provides for the distribution and settlement of electronic credits and debits among a large number of financial institutions. The acquiring processor may be a financial institution or a third party processor. The acquiring processor communicates with an issuing financial institution 40 or a card issuer 44. The merchant may also optionally communicate with a PIN confirmation and fraud prevention system 48 (e.g., CyberSource, CyberCash, Digital Identification), or other method of verifying the identity of the purchaser and the validity of the purchase. In alternate embodiments of the present invention, a service organization called an alias account facilitator 52 may communicate with the merchant. Additionally, the alias account facilitator may communicate with the acquiring processor 38, or the issuing financial institution. The merchant may send packages via a shipping system 59. The shipping system may also communicate with the alias account facilitator. The shipping system may include a private

postal store such as Mail Box, Etc., a postal box located at a U.S. Postal Station, or a private shipper such as United Parcel Service (UPS) or Federal Express (FEDEX). In the preferred embodiment, all the components shown in FIG.2 are connected through a data network such as the Internet and may utilize encryption techniques such as Secure Sockets Layer (SSL) or
5 Secure Electronic Transaction (SET).

FIGs. 3A and 3B are flow charts outlining the steps for processing a credit card transaction utilizing an alias account in the preferred embodiment of the present invention. With reference to FIGs. 2, 3A, 3B, and 3C, the steps of the method will now be described. Beginning with step 70, the purchaser 30 orders an item utilizing an alias account name and
10 number. The purchaser may purchase via the Internet, telephone, in person, or via mail. In step 72, the merchant receives the order from the purchaser. In step 74, the merchant may optionally verify the identity of the purchaser by requesting a personal identification number (PIN) from the purchaser. The PIN is then verified via the PIN confirmation and fraud prevention system 48. Next in step 76, the merchant requests authorization of the transaction
15 using the alias account from the acquiring processor 38. In step 78, the acquiring processor, utilizing the ACH Network, requests authorization from the issuing financial institution 40 or, if required, the card issuer 44. In many instances, the issuing financial institution, such as a bank, is actually a credit card issuer. In other cases, the credit card is issued by a separate card issuer (e.g., American Express). In step 80, the card issuer or the issuing financial institution
20 replies to the authorization request to the acquiring processor. The reply will include either an acceptance of the credit transaction or a rejection of the credit transaction. Next, in step 82 (FIG. 3B), the acquiring processor forwards the authorization response to the merchant.

In step 84, it is determined by the merchant if the credit transaction is accepted. If the credit card transaction is accepted, the method moves to step 86, where the merchant sends the
25 ordered item(s) to the purchaser. The ordered item may optionally be delivered via the shipping system 59 to an alias address associated with the alias name of the purchaser. The alias address may be located at a private postal store or at a remote location away from the purchaser, such as a postal box located at a U.S. Postal Station, requiring the pickup of the ordered item by the purchaser. Alternately, the ordered item may be sent via a blind shipment
30 to a private shipping company. The merchant sends the ordered item to the private shipping company with the purchaser's alias account number. The private shipping company then

communicates with the alias account facilitator to obtain the desired shipping address of the purchaser, which may be the purchaser's actual address or an alias address.

If, however, it is determined that the credit transaction is rejected, the method moves from step 84 to step 88, where the merchant rejects the purchaser's order.

5 The method described in FIGs. 3A and 3B illustrates the credit card transaction in which the financial institution or card issuer associates and tracks the alias account with the primary core account. All information utilized in the purchase order utilizes only the alias account information, thereby maintaining the privacy of the purchaser by masking the true identity of the purchaser 30.

10 FIGs. 4A and 4B are flow charts outlining the steps for processing a alias credit card transaction through the alias account facilitator 52. With reference to FIGs. 2, 4A, and 4B, the steps of the method will now be described. Beginning with step 90, the purchaser 30 orders an item utilizing an alias account name and number. The purchaser may buy through the Internet, telephone, mail, or in person. In step 92, the merchant receives the order from the
15 purchaser. In step 94, the merchant may optionally verify the identity of the purchaser by requesting a personal identification number (PIN) from the purchaser. The PIN is then verified via the PIN. Next, in step 96, the merchant sends the credit transaction order to the alias account facilitator 52. In step 98, the alias account facilitator strips the alias account information from the credit card transaction order and replaces the information with the
20 primary core account information. Then, in step 100, the modified credit transaction order is sent to the acquiring processor 38.

In step 102 (FIG. 4B), the acquiring processor, utilizing the ACH Network, requests authorization from the issuing financial institution 40 or, if required, the card issuer 44. In step 104, the card issuer or the issuing financial institution replies to the authorization request
25 to the acquiring processor. The reply will include either an acceptance of the credit transaction or a rejection of the credit transaction. Next, in step 106, the acquiring processor will forward the authorization response to the merchant.

In step 108, it is determined by the merchant if the credit transaction is accepted. If the credit transaction is accepted, the method moves to step 110 where the merchant sends the
30 ordered item(s) to the purchaser. The ordered item may optionally be delivered via shipping system 59 to an alias address associated with the alias name of the purchaser. The alias address may be located at a private postal store or at a remote location such as a postal box

located at a U.S. Postal Station, requiring the pickup of the ordered item by the purchaser. Alternately, the ordered item may be sent via a blind shipment to a private shipping company. The merchant sends the ordered item to the private shipping company with the purchaser's alias account number. The private shipping company then communicates with the alias
5 account facilitator to obtain the desired shipping address of the purchaser, which may be the purchaser's actual address or an alias address.

If, however, it is determined that the credit card transaction is rejected, the method moves from step 108 to step 112, where the merchant rejects the purchaser's order.

The method described in FIGs. 4A and 4B illustrates a credit card transaction utilizing
10 the alias account facilitator to associate the alias credit card account with the primary core account. The card issuer or issuing financial institution still tracks the primary core account, but is unaware of the alias account information. Since the alias account facilitator is the only institution which can associate the correct primary core account with the alias account of the purchaser, privacy is insured solely by the alias account facilitator.

FIGs. 5A and 5B are flow charts outlining the steps for processing a alias credit card
15 transaction through the alias account facilitator 52 acting as an Independent Service Organization (ISO) in an alternate embodiment of the present invention. With reference to FIGs. 2, 5A, and 5B, the steps of the method will now be described. Beginning with step 120, the purchaser 30 orders an item utilizing an alias account name and number. The purchaser
20 may purchase via the Internet, telephone, mail, or in person. In step 122, the merchant receives the order from the purchaser. In step 124, the merchant may verify the identity of the purchaser by requesting a PIN from the purchaser. The PIN is then verified via the PIN confirmation system 48. Next in step 126, the merchant sends the credit card transaction order to the alias account facilitator 52. In step 128, the alias account facilitator strips the alias
25 account information from the credit card transaction order and replaces the information with the primary core account information.

In step 130, the alias account facilitator 52, utilizing the ACH Network, requests authorization from the issuing financial institution 40 or, if required, the card issuer 44, thereby functioning as an ISO. An ISO performs sale and/or service transactions on behalf of
30 the issuing financial institution 40 or the acquiring processor 38. In step 132 (FIG. 5B), the card issuer or the issuing financial institution replies to the authorization request to the alias account facilitator. The reply will include either an acceptance of the credit card transaction

or a rejection of the credit card transaction. Next, in step 134, the alias account facilitator will forward the authorization response to the merchant.

In step 136, it is determined by the merchant if the credit card transaction is accepted. If the credit card transaction is accepted, the method moves to step 138 where the merchant
5 sends the ordered item(s) to the purchaser. The ordered item may optionally be delivered via shipping system 59 to an alias address associated with the alias name of the purchaser. The alias address may be located at a private postal store or at another remote location such as a postal box located at a U.S. Postal Station, requiring the pickup of the ordered item by the purchaser. Alternately, the ordered item may be sent via a blind shipment to a private shipping
10 company. The merchant sends the ordered item to the private shipping company with the purchaser's alias account number. The private shipping company then communicates with the alias account facilitator to obtain the desired shipping address of the purchaser, which may be the purchaser's actual address or an alias address.

If, however, it is determined that the credit card transaction is rejected, the method
15 moves from step 136 to step 140, where the merchant rejects the purchaser's order.

The method of FIGs. 5A and 5B describes a credit card transaction utilizing the alias account facilitator to associate the alias credit card account with the primary core account. The alias account facilitator also acts as the ISO, obtaining authorization via the ACH network. The card issuer or financial institution still tracks the primary core account, but is unaware of
20 the alias account information. Since the alias account facilitator is the only institution which can associate the correct primary core account with the alias account of the purchaser, privacy is insured solely by the alias account facilitator.

FIGs. 6A and 6B are flow charts outlining the steps for establishing an alias account by the purchaser 30 having an existing account in the preferred embodiment of the present
25 invention. With reference to FIGs. 2, 6A, and 6B, the steps of the method will now be described. Beginning with step 150, the purchaser communicates with the alias account facilitator 52. In the preferred embodiment of the present invention, the purchaser communicates through a web site of the alias account facilitator via a secure link to the Internet. The alias account facilitator web site may be reached by going directly to the site or
30 through a hyperlink associated with another web site, such as a banking institution or Internet banner advertisement. However, in alternate embodiments, the purchaser may communicate by telephone, mail, or in person. Next, in step 152, the alias account facilitator requests

information regarding the purchaser and his existing account. In step 154, the purchaser sends the information to the alias account facilitator. Then, in step 156, the alias account facilitator creates alias information associated with the existing account (primary core account) of the purchaser. The alias information may include an alias name, address, and PIN number. Alias names, in the preferred embodiment of the present invention, are typically generated in a series of 1000 accounts per series (e.g., Roberts series would have Roberts1000 through Roberts2000). In an alternate embodiment of the present invention, the customer may select his own alias, within certain prescribed parameters. A series number is then added to the customer's selected name. In still another alternate embodiment, any series of symbols or numbers may be used to form an alias name.

The purchaser may optionally request an alias address to which an ordered item may be sent. The alias address may be located at a private postal store or at any remote location such as a postal box located at a U.S. Postal Station, requiring the pickup of the ordered item by the purchaser. A convenient location of the alias address may be selected by the purchaser, such as the nearest private postal store. Alternately, the ordered item may be sent via a blind shipment to a private shipping company. When a blind shipment is made, the merchant sends the ordered item to the private shipping company with the purchaser's alias account information. The purchaser may request delivery via private shipping company. The purchaser must select the desired location where the ordered item is to be delivered, such as a home address or a postal box. The creation of an alias address may be done at the time of establishing an alias account or a later time by the alias account facilitator. The alias account facilitator may store the alias address with the other alias information of the purchaser.

Next, in step 158, the alias account facilitator sends the alias information and the existing account information to the issuing financial institution 40 or card issuer 44 for verification. In step 160 (FIG. 6B), the issuing financial institution or card issuer verifies current account information of the purchaser 30. In step 162, it is determined by the issuing financial institution or card issuer whether the existing account is valid. If the existing account is not valid, the method moves to step 164 where the issuing financial institution or card issuer sends a rejection to the alias account facilitator. Next, in step 166, the alias account facilitator sends an invalid account notice to the purchaser.

However, if it is determined that the existing account is valid, the method moves from step 162 to step 168 where the issuing financial institution or card issuer creates an alias

parallel account associated with the existing account. Next, in step 170, the issuing financial institution or card issuer sends the alias account information to the alias account facilitator. In step 172, the alias account facilitator sends the alias account information to the purchaser by e-mail, a secure Internet web page, postal service, or direct delivery. If a PIN is utilized in the alias account, the PIN

is sent separately from the alias account information for added security. Any of the information items of the alias account information may also be sent separately to ensure added levels of security. Additionally, if the purchaser desires a physical credit card, the issuing financial institution or card issuer sends a physical card to the purchaser.

FIGs. 7A, 7B, and 7C are flow charts outlining the steps for establishing an alias account by the purchaser 30 requiring a primary core account. With reference to FIGs. 2, 7A, 7B, and 7C, the steps of the method will now be described. Beginning with step 180, the purchaser communicates with the alias account facilitator 52. As described in FIG. 6, communication may take the form of mail, telephone, via Internet, or in person. Next, in step 182, the alias account facilitator requests information of the purchaser necessary for establishing a credit account. In step 184, the purchaser sends the requested information to the alias account facilitator. Then, in step 186, the alias account facilitator creates alias information. The alias information may include an alias name, address, and PIN.

Next, in step 188, the alias account facilitator sends the alias information and the purchaser information to the issuing financial institution 40 or card issuer 44 for verification, credit check, and account set-up. In step 190 (FIG. 7B), the issuing financial institution or card issuer verifies the data of the purchaser 30. In step 192, it is determined by the issuing financial institution or card issuer if the purchaser has proper identification and acceptable credit for the establishment of a credit account. If a new account is rejected for the purchaser, the method moves to step 194 where the issuing financial institution or card issuer sends a rejection to the alias account facilitator. Next, in step 196, the alias account facilitator sends a rejection notice to the purchaser.

However, if it is determined that the application of the purchaser 30 is accepted, the method moves from step 192 to step 198 where the issuing financial institution or card issuer creates both a new primary core account and an alias parallel account associated with the primary core account. In an alternate embodiment, only an alias account is created, without a core account. Next, in step 200, the issuing financial institution or card issuer sends the alias

account information to the alias account facilitator. In step 202, the alias account facilitator sends the alias account information to the purchaser by e-mail, a secure Internet web page, postal service, or direct delivery. If a PIN is utilized in the alias account, the PIN is sent separately from the alias account information for added security. Any of the information items of the alias account information may also be sent separately to ensure added levels of security. Additional, if the purchaser desires a physical credit card, the issuing financial institution or card issuer sends a physical card to the purchaser.

FIG. 8 is a top level diagram illustrating a system configuration of an alias account system 220 in the preferred embodiment of the present invention. The alias account system includes the alias account facilitator 52 having a plurality of data connections 222 to a plurality of providers 224, issuing financial institutions 40, and provider data hosts 226. The alias account facilitator may be located at a host site having a secure server 228 (e.g., Electronic Data Systems). The data connections may be dedicated or dial-up connections. The plurality of providers 224 and issuing financial institutions 40 are credit card issuers. Some of the providers 224 may include provider data hosts 226 which host the database of a corresponding provider 224. In the preferred embodiment of the present invention, the data transmitted between the alias account facilitator and the issuing financial institutions and the providers is encrypted for security.

FIG. 9 is a diagram of high level information transfer by the alias account system 220 in the preferred embodiment of the present invention.

Data may be sent a variety of ways to include communications with an object based database 230 or a DB2 based database 232. Additionally, data may be transferred via the Internet to an institution's Internet server 234 which accesses an institution's core database 236. In the preferred embodiment of the present invention, communication between the alias account facilitator 52 and the various institutional databases is done over a dedicated encrypted communications link.

When the alias account facilitator 52 communicates with the object based database 230, a proxy server 240 utilizing an object-based computer language, such as CORBA is used. The proxy server may signal the database 230 by sending an object request to record message 242. The database may respond by sending an acknowledge and open record message 244 to the proxy server. Next, the proxy server may send an action to account message 246 to the database. The database may then respond by sending a confirmation and close record message

248 to the proxy server. In an alternate method, a CORBA object from the proxy server may contain the record message 242, open record message 244, and action to account message 246 all in one object. The database would then only respond with a confirmation; and close record message 248 or an invalid account message to the proxy server.

5 When the alias account facilitator 52 communicates with the institution's core database 236 via the Internet, a web server 250 using HTML or XML communicates with the institution's Internet server 234. An HTML page 252 or XML object is sent between the web server and the institutions Internet server to communicate.

10 When the alias account facilitator 52 communicates with the DB2-based database 232, a DB2-based proxy server 254 is used. The proxy server signals the database 232 by sending a request to open record message 256. The database responds by sending an acknowledge and open record message 258 to the proxy server. Next, the proxy server sends an action to account message 260 to the database. The database then responds by sending a confirmation and close record message 262 to the proxy server.

15 There are several different types of accounts which may be established with an existing credit card account. An existing credit card account may be converted to an alias account in which the existing credit card (real identity) is canceled and replaced with an alias name and account number. An alias account may be an affinity card account in which the alias account includes an affiliation with an organization (e.g., alma mater, sports team, retailer, etc.). The
20 alias account may include both an alias name and a completely different account number from the existing primary account or the same account number as the existing primary account. The alias account may be established as a core account linked to another core account via an identification tag.

25 When a purchaser does not have an existing credit card core account and a new credit card account must be establish, several options exist in the creation of an alias account. A purchaser may establish only an alias account without creating a new primary core account with the purchaser's true identity. The alias account may be an affinity card account associated with an organization. The alias account may include the same or a different account number as a primary core account having the purchaser's real identity. The alias account may
30 also be a core account linked to another core account via an identification tag.

 The alias account may include a virtual card and/or a physical card. A virtual card includes the alias information of the purchaser and an expiration date, that may be stored on

any medium, including a digital medium (e.g., computer, set top box, Internet appliance, wireless phone or other wireless device), without any physical card. The alias account may be associated with a physical card which may include a photo identification for verification of the individual as the true purchaser when making live purchases. To further enhance the individual's privacy while ensuring against fraudulent purchases on the alias account, the physical card may be two separate cards. A first card may be an official identification card with a photograph of the purchaser. The second card may be a card used for purchases or other purposes. The alias account may be a debit card, credit card, automated teller machine (ATM) card, electronic cash card, smart card, digital check, medical/prescription card, or any other form of medium used to conduct transactions/sales.

In an alternate embodiment of the present invention, the purchaser may request specific marketing information resulting from the credit card transactions be sent to the purchaser. During the creation of an alias account, the purchaser may select various types or subjects of marketing ads which the purchaser wishes to be sent to the purchaser. The alias account facilitator 38 may filter the desired marketing information out from the unwanted material and deliver the selected material directly to the purchaser (via e-mail, mail, or telephone) or to an alias address.

The method described above offers many advantages over existing credit card transactions. The method provides privacy for a purchaser using a credit card. By masking the true identity of the purchaser, the purchaser avoids unwanted solicitations. Additionally, personal information, including the spending habits of the purchaser, is held only by those parties needing information during the credit card transaction. The method also prevents identity theft by providing an alias which cannot be used for identifying a specific individual. By utilizing the described invention, more purchasers are encouraged to purchase items, especially via the Internet, through the use of credit cards.

In an alternate embodiment, the present invention may be used in medical transactions. Currently, medical cards are utilized by patients when seeking medical assistance at a hospital, health care provider, or making a purchase at a pharmacy or other health care related merchant. The medical cards typically contain information on the patient's medical insurer, medical insurance data, and other relevant information for the payment of services. FIG. 10 is a block diagram illustrating a medical transaction of a purchaser 300 utilizing an alias account in accordance with the teachings of the present invention. The purchaser 300 communicates with

a health care provider 302, such as a hospital, physician, pharmacist, or other health related institution or merchant. The purchaser is an individual purchasing medical services or goods, typically a patient, insured individual, or head of family to which the medical services are charged. The purchaser may utilize a medical card having an alias name, account or member number, group number, and other information similar to the alias credit card discussed above. The health care provider then communicates with an acquiring processor 304 to obtain authorization of the transaction order of the purchaser and any necessary coverage information on the purchaser. The acquiring processor, utilizing a health insurance network similar to the ACH network, requests purchase or coverage authorization and other coverage information from a financial institution 306. The financial institution is any organization which handles the health account of the purchaser, such as a health insurance company, plan administrator, health maintenance organization (HMO), or some other service organization storing the information of the purchaser.

The financial institution 306, matches the alias name and account of the purchaser 300 with the core name and account and responds by sending the coverage or purchase authorization and any other coverage information necessary for the medical transaction to the acquiring processor 304. The acquiring processor then sends the information to the health care provider 302.

If, however, it is determined that the authorization is rejected, the health care provider 302 rejects the purchaser's service or product purchaser request.

In an alternate embodiment, the health care provider may send a request for coverage authorization or coverage information to an alias account facilitator 308. The alias account facilitator can then determine the core account corresponding to the purchaser 300 and request information from the acquiring processor 304. The acquiring processor then requests information from the financial institution 306. The alias account facilitator may act as an ISO and request information directly from the financial institution. The financial institution then sends the requested information back via the alias account facilitator to the health care provider.

Alternatively, the purchaser 300 may establish an alias health account associated with the purchaser. The alias health account may include an alias name masking the true identity of the purchaser and may also include an alias account or member number, an alias address, an alias group number, and an alias PIN. The purchaser then conducts a medical transaction

with the health care provider 302 to purchase a selected item or service using the alias account, in a manner similar to the methods described in FIGs. 3-5. This transaction may or may not include the use of a physical credit card. The alias account is then verified as a valid account (either via the alias account facilitator 308 or the acquiring processor 304) to the financial institution 306. The alias account facilitator or acquiring processor then verifies that sufficient coverage or credit is available to purchase the selected item or service from the financial institution. The alias account is associated with a core account displaying the true identity of the purchaser. The transaction is then recorded and may be debited to the core account.

Still referring to FIG. 10, the purchaser 300 may also use an alias name when transferring medical records from a first primary health care provider 302 to a secondary health care provider 309. The health care provider 302 may transfer the medical records to the alias account facilitator 308 who replaces the true identity of the purchaser with an alias name. The records are then transferred to the second health care provider 309. The medical records, with associated history, may then be examined by the second health care provider 309, without knowing the true identity of the purchaser. In addition, when the patient is examined by the second health care provider 309, the purchaser uses the alias name associated with the aliased medical records, thereby keeping the privacy of the purchaser, while still providing all the relevant information necessary for the second health care provider to treat the purchaser.

The method described in FIG. 10 offers advantages over existing medical systems. The purchaser's privacy is maintained by providing a health care provider with alias information, preventing the transfer of personal information, while still allowing the health care provider a method of verifying the coverage of their patients. In addition, the card may be used at participating pharmacies or other health care related merchants, allowing the anonymous procurement of prescribed drugs and other prescribed health products and services.

An alias account may also be utilized in conjunction with flexible spending accounts. Many employers use flexible spending accounts for medical and child care expenses. An employee directs a specific amount of the employee's wages be sent to the flexible spending account. The employee, after paying the child care or medical expense incurred, may submit a request for reimbursement from the flexible spending account. By using a flexible spending account, the employee is not taxed on wages which are placed within the flexible spending account. In an alternate embodiment of the present invention, the employee may give an alias name and number to the health care provider or a child care provider. The health care provider

or child care provider can then submit a request for payment from the alias account facilitator. The alias account facilitator may then request transfer of funds from the employee's flexible spending account to the health care provider or child care provider via the employer or employer's plan administrator. By utilizing an alias account, the employee does not have to give personal information to the health care provider or child care provider. Additionally, payment is simplified for the employee since the employee does not have to submit paperwork to request reimbursement.

In still another alternate embodiment, the credit status of an individual necessary to complete a purchase may be examined by utilizing an alias name and account. In existing systems, a customer requesting credit or verifying credit worthiness to complete a purchase, such as for a home mortgage or telephone service, must submit personal information to a financial institution, such as a mortgage company to obtain credit approval. The financial institutions may include banks, mortgage companies, utility companies, merchants, or telephone companies. Many times, the financial institutions compile information on customers, and sells the information to marketing agencies. To prevent the transfer of this personal information, while still providing the financial institution with a method of verifying the credit rating of the customer, an alias name and account may be utilized. FIG. 11 is a block diagram illustrating a transaction for determining a credit status of a customer utilizing an alias account in accordance with the teachings of the present invention. The customer requests a transaction requiring a credit status check of the customer from a financial institution. The financial institution may be any organization to which a customer must provide his credit status to complete a requested transaction, such as a bank, mortgage company, utility company, merchant, or telephone company. The financial institution requests a credit report from an alias account facilitator. The alias account facilitator matches the alias name and account with the true identity of the customer. The alias account facilitator then requests a credit report for the customer from a credit bureau (e.g., Equifax, Experian, Trans Union, etc.) which maintains detailed credit reports on individuals. The credit bureau then responds by sending the requested credit report to the alias account facilitator. The alias account facilitator then sends the credit report to the financial institution with the true identity removed from the credit report. The financial institution then determines whether to provide the requested credit to the customer.

Still referring to FIG. 11, the customer 310 may also provide various financial institutions 312 with information on an alias saving account(s). The savings account may be associated with a core account having the true identity of the customer. However the alias savings account includes an alias name and optional alias address, thereby providing
5 anonymity to the customer when providing the savings account information to the financial institution.

By utilizing the method described in FIG. 11, a customer may receive a credit check from a financial institution without providing personal information to the financial institution. By preventing the financial institution from determining the true identity of a customer, the
10 customer's privacy is maintained.

It is thus believed that the operation and construction of the present invention will be apparent from the foregoing description. While the method shown and described has been characterized as being preferred, it will be readily apparent that various changes and modifications could be made therein without departing from the scope of the invention as
15 defined in the following claims.

WHAT IS CLAIMED IS:

1. A method of masking a true identity of a purchaser (30) during a credit transaction, the method comprising the steps of:

establishing an alias credit account associated with the purchaser, the alias

5 credit account masking the true identity of the purchaser;

conducting a credit transaction by the purchaser to purchase a selected item using the alias credit account; and

associating the alias credit account with the purchaser.

2. The method of masking a true identity of a purchaser of claim 1 wherein the
10 step of associating the alias credit account with the purchaser includes associating the alias credit account with a core account having the true identity of the purchaser.

3. The method of masking a true identity of a purchaser of claim 2 wherein the step of associating the alias credit account with a core account includes debiting the core account for the credit card transaction.

15 4. The method of masking a true identity of a purchaser of claim 2 wherein the step of associating the alias credit account with a core account includes linking, by a service organization, the alias credit account with the core account.

5. The method of masking a true identity of a purchaser of claim 4 wherein the step of linking, by a service organization, the alias credit account with the core account
20 includes stripping alias information from the alias account and replacing the stripped alias information with information from the core account.

6. The method of masking a true identity of a purchaser of claim 4 further comprising, after the step of associating the alias credit account with a core account, the steps of:

25 receiving, in the service organization, a plurality of marketing advertisements in association with the credit transaction;

transmitting, by the purchaser to the service organization, selected marketing advertisements for the purchaser;

30 filtering, by the service organization, the selected marketing advertisements for the purchaser; and

sending the selected marketing advertisements to the purchaser.

7. The method of masking a true identity of a purchaser of claim 1 wherein the alias credit account displays alias information masking the true identity of the purchaser.

8. The method of masking a true identity of a purchaser of claim 7 wherein the alias information includes an alias name and an alias account number.

5 9. The method of masking a true identity of a purchaser of claim 8 wherein the alias information includes an alias address for the purchaser.

10. The method of masking a true identity of a purchaser of claim 8 further comprising, after the step of associating the alias credit account with the purchaser, the step of delivering the selected item to the alias address.

10 11. The method of masking a true identity of a purchaser of claim 1 wherein the alias credit account includes a virtual card having an alias name and alias account number.

12. The method of masking a true identity of a purchaser of claim 1 wherein the alias credit account includes a physical card having an alias name and alias account number.

15 13. The method of masking a true identity of a purchaser of claim 12 wherein the physical card includes a photograph of the purchaser to verify the purchaser.

14. The method of masking a true identity of a purchaser of claim 1 wherein the step of conducting a credit card transaction by the purchaser includes authorizing the transaction.

20 15. The method of masking a true identity of a purchaser of claim 14 wherein the step of authorizing the transaction includes:

requesting a credit status report on the purchaser by a merchant selling to the purchaser in the transaction;

associating the alias account with the true identity of the purchaser; and

sending the credit status report of the purchaser to the merchant.

25 16. The method of masking a true identity of a purchaser of claim 14 wherein the step of authorizing the transaction includes: verifying the alias account as a valid credit account; and verifying that credit is available to purchase the selected item.

30 17. The method of masking a true identity of a purchaser of claim 1 further comprising, after the step of associating the alias credit account with the purchaser, the step of delivering the selected item to the purchaser.

18. The method of masking a true identity of a purchaser of claim 17 wherein the step of delivering the selected item to the purchaser includes:

delivering the selected item to a shipping company;
associating the alias account with a desired address of the purchaser; and
delivering the selected item to the desired address.

19. The method of masking a true identity of a purchaser of claim 17 wherein the
5 desired address is an alias address for pickup of the selected item by the purchaser.

20. The method of masking a true identity of a purchaser of claim 1 wherein the
step of enacting a credit card transaction by the purchaser includes verifying the purchaser
through a Personal Identification Number (PIN) confirmation system.

21. A method of conducting an anonymous credit card transaction by a purchaser
10 (30), the method comprising the steps of:

ordering a selected item by the purchaser, the purchaser utilizing an alias credit
account having alias information of the purchaser, the alias credit account associated with a
core account having a real identity of the purchaser;

15 authorizing a purchase of the selected item; and
sending the selected item to the purchaser.

22. The method of conducting an anonymous credit transaction of claim 22,
wherein the step of authorizing a purchase of the selected item includes verifying the alias
account as valid and having allowable credit to purchase the selected item.

23. The method of conducting an anonymous credit transaction of claim 22,
20 wherein the step of verifying the alias account includes linking the alias account with the core
account of the purchaser through a service organization.

24. The method of conducting an anonymous credit transaction of claim 23 wherein
the service organization alone maintains a database for associating the alias credit account with
the core account.

25. The method of conducting an anonymous credit transaction of claim 21 wherein
the step of sending the selected item to the purchaser includes the step of delivering the
selected item to an alias address for pickup by the purchaser.

26. The method of conducting an anonymous credit transaction of claim 21 wherein
the step of sending the selected item to the purchaser includes the steps of:

30 delivering the selected item to a shipping company;
associating the alias account with a desired address of the purchaser; and
delivering the selected item to the desired address.

27. A method of masking a true identity of a purchaser (30) during a credit transaction, the method comprising the steps of:

establishing an alias credit account associated with the purchaser, the alias credit account having an alias name masking the true identity of the purchaser;

5 conducting a credit transaction by the purchaser to purchase a selected item using the alias account;

verifying that the alias account is a valid credit account and that credit is available to purchase the selected item;

10 associating the alias credit account with a core account displaying the true identity of the purchaser; and

debiting the core account for the credit transaction.

28. The method of masking the identity of a purchaser of claim 27, further comprising, after the step of associating the alias credit account with a core account, the step of delivering the selected item to a desired address of the purchaser.

15 29. A method of masking a true identity of an individual (30) during a transaction, the method comprising the steps of:

establishing an alias account associated with the individual, the alias account masking the true identity of the individual;

20 conducting a transaction by the individual using the alias account; and associating the alias account with the individual.

30. The method of masking a true identity of an individual of claim 29 wherein: the individual is a patient;

the step of conducting a transaction includes:

25 treating a patient, by a health care provider; and

requesting information on health insurance coverage of the patient by the health care provider; and

the step of associating the alias account with the individual includes linking the alias account to the true identity of the individual.

31. The method of masking a true identity of an individual of claim 30 further comprising, after the step of associating the alias account with the individual, the step of transmitting the requested information of the patient to the health care provider.

32. The method of masking a true identity of an individual of claim 29 wherein:

the alias account is associated with a flexible spending account of the individual; and

the step of conducting a transaction by the individual includes:

providing a benefits provider providing benefits to the individual with
5 information from the alias account; and

requesting payment from the alias account by the benefits provider.

33. The method of masking a true identity of an individual of claim 32 further comprising, after the step of associating the alias account with the individual, the step of paying the benefits provider from the alias account.

10 34. The method of masking a true identity of an individual of claim 29 wherein: the individual is a purchaser;

the step of conducting a transaction includes:

purchasing through the alias account by the purchaser from a health care merchant; and

15 requesting information on health coverage of the purchaser by the health merchant; and

the step of associating the alias account with the purchaser includes linking the alias account to the true identity of the purchaser.

20 35. The method of masking a true identity of an individual of claim 34 wherein the health care merchant provides medical services during the transaction.

36. The method of masking a true identity of an individual of claim 34 wherein the health care merchant provides medical goods to the purchaser during the transaction.

37. The method of masking a true identity of an individual of claim 29 wherein: the individual is a purchaser;

25 the step of conducting a transaction includes:

purchasing through the alias account by the purchaser from a health care merchant; and

verifying that the alias account is a valid credit account and that credit is available to purchase the selected item.

30 38. A method of masking a true identity of an individual (300) during a transfer of medical records of the patient from a first health care provider (302) to a second health care provider (309), the method comprising the steps of:

transferring the medical records from the first health care provider to a service organization (308);

masking the true identity of the individual by the service organization; and
transferring the masked medical records to the second health care provider.

5 39. The method of masking a true identity of an individual of claim 38 wherein the step of masking the true identity of the individual by the service organization includes the step of replacing the true identify of the individual with an alias name.

 40. A method of masking a true identity of an individual (310) requiring a credit status report to complete a transaction, the method comprising the steps of:

10 establishing an alias account associated with the individual;
 conducting the transaction by the individual to a financial institution (312)
using the alias account, the transaction requiring the credit status report;
 requesting the credit status report by the financial institution;
 associating the alias account with the individual; and
15 sending the credit status report of the individual to the financial institution.

1/15

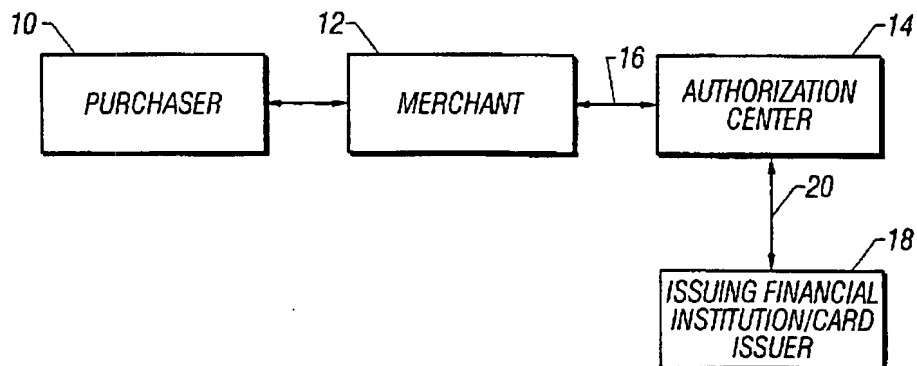


FIG. 1
(Prior Art)

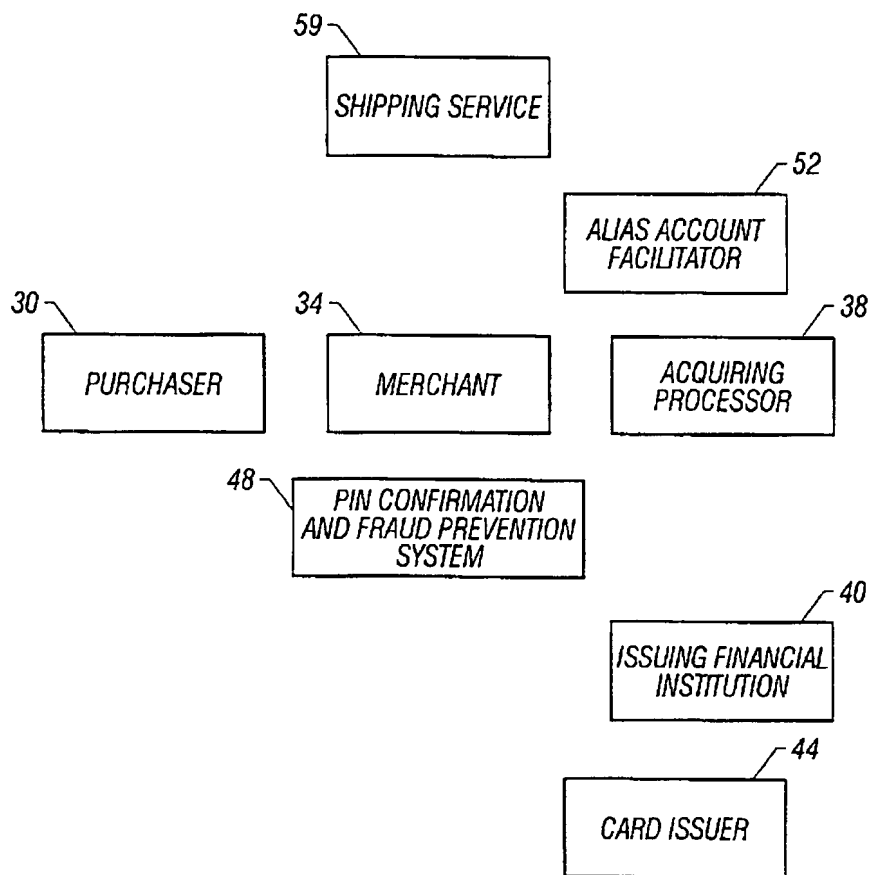
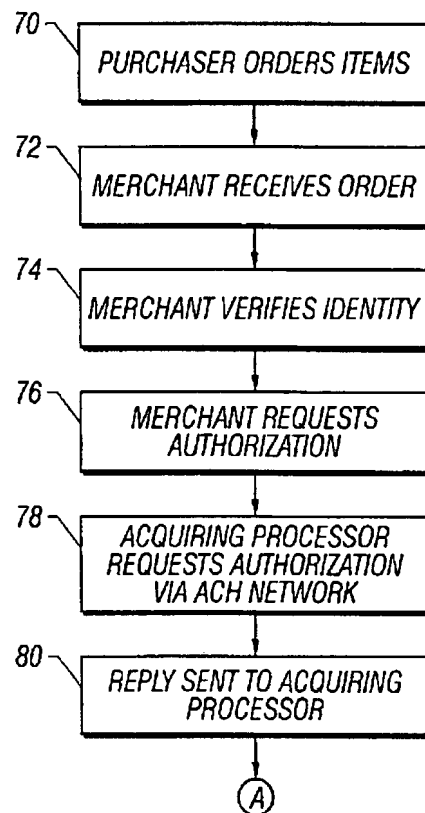


FIG. 2

2/15



TO FIG. 3B

FIG. 3A

3/15

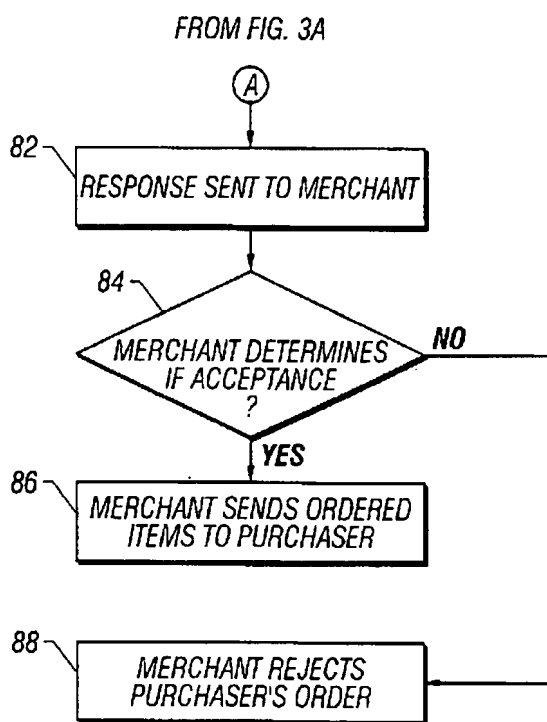
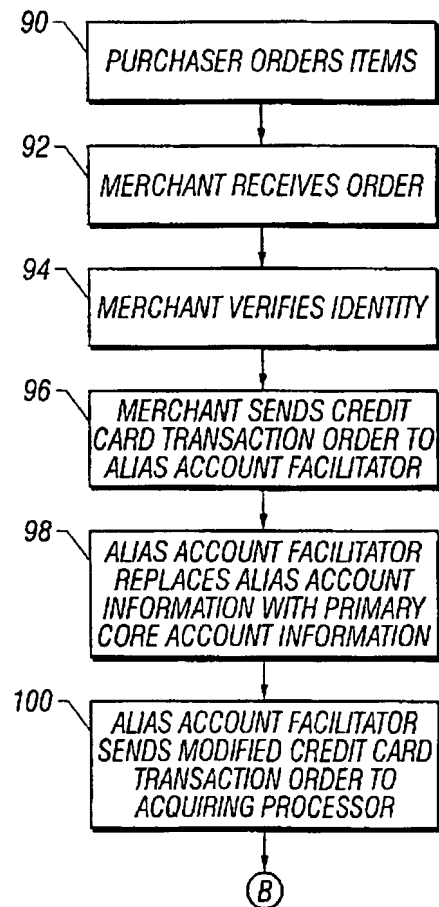


FIG. 3B

4/15



TO FIG. 4B

FIG. 4A

5/15

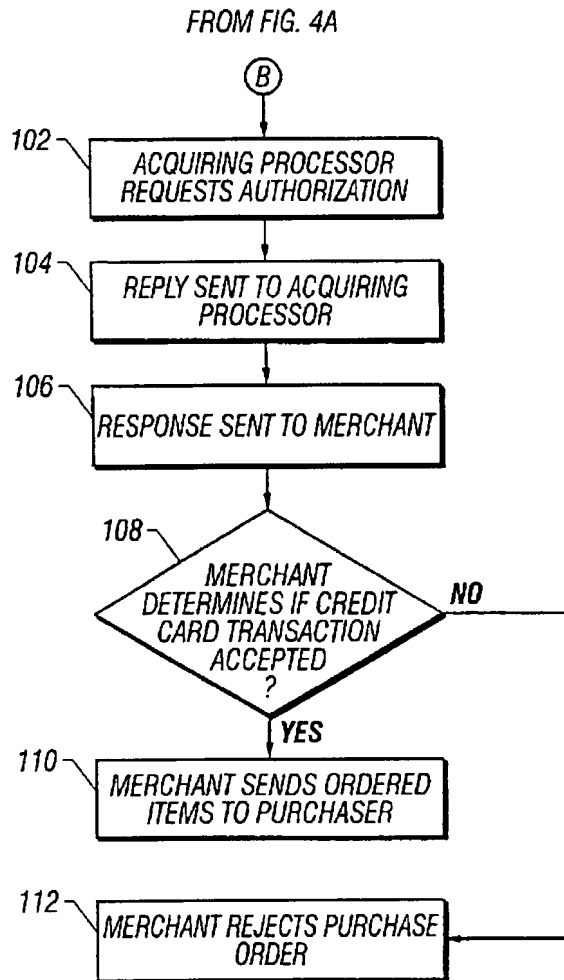
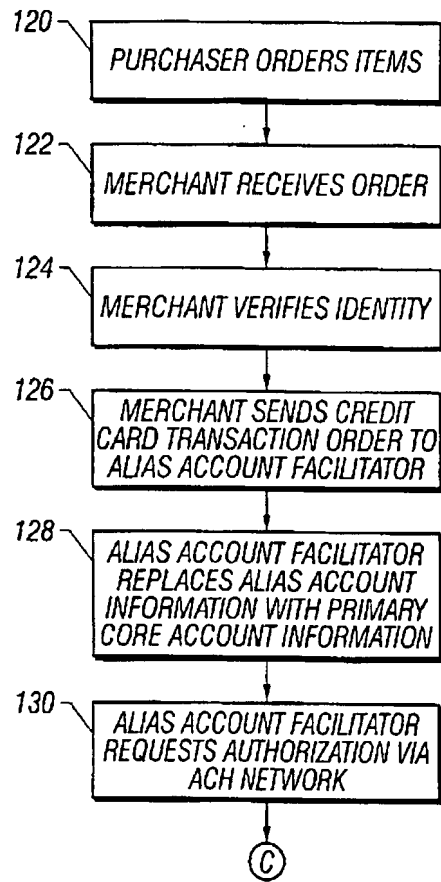


FIG. 4B

6/15



TO FIG. 5B

FIG. 5A

7/15

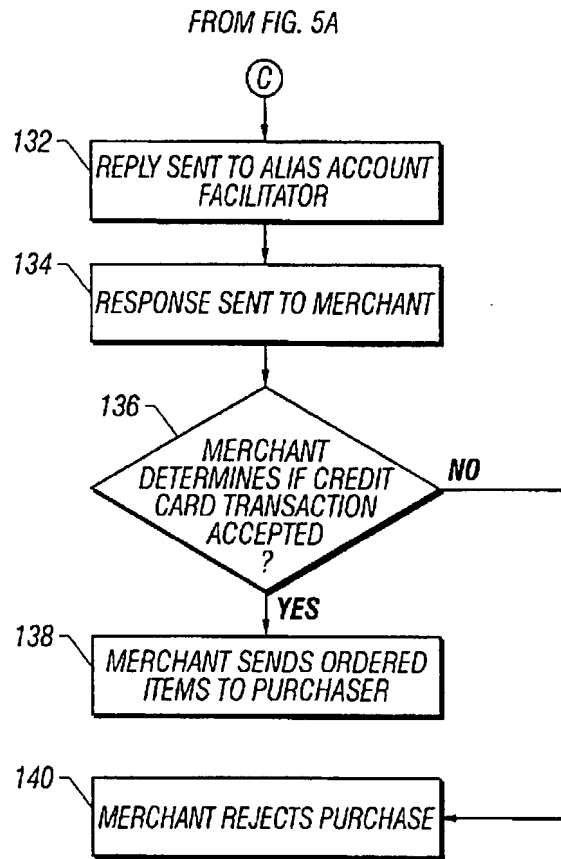
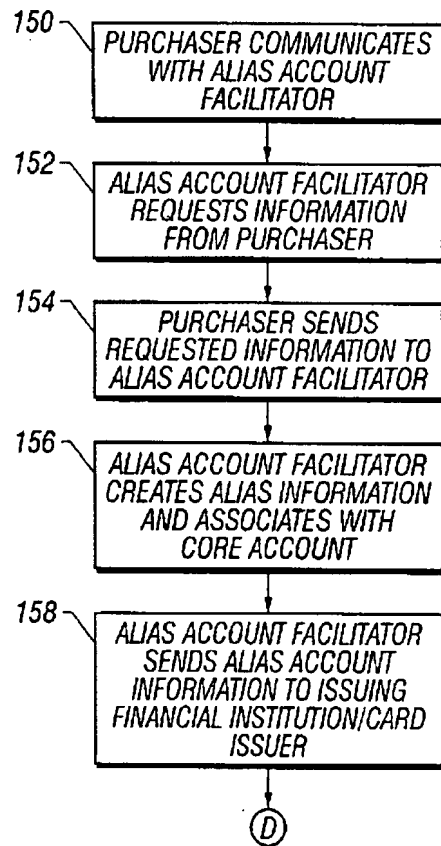


FIG. 5B

8/15



TO FIG. 6B

FIG. 6A

9/15

FROM FIG. 6A

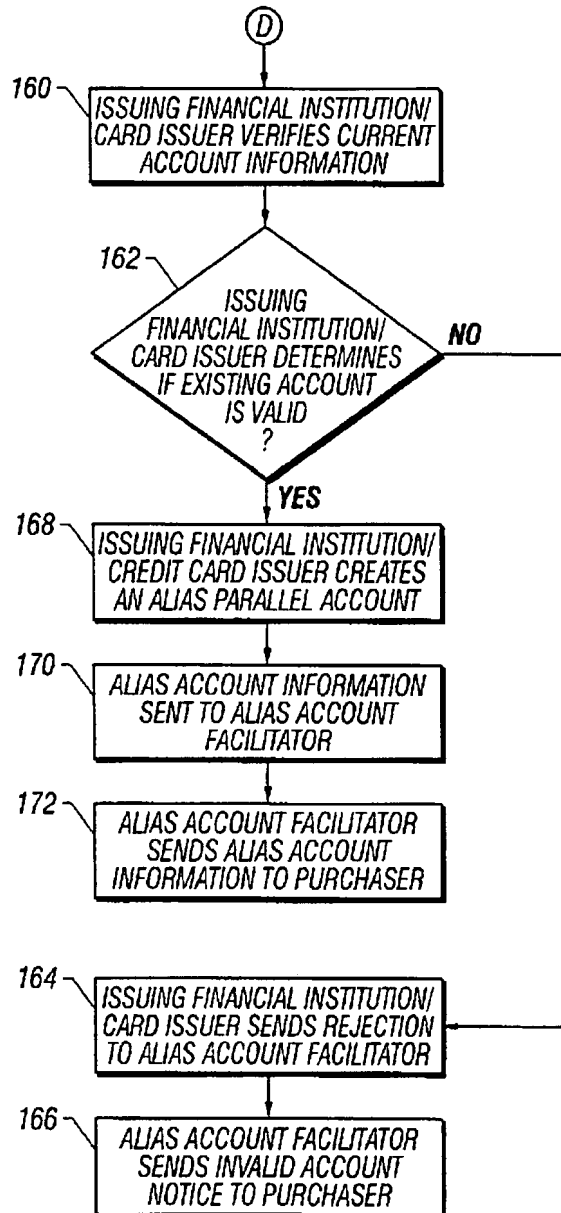
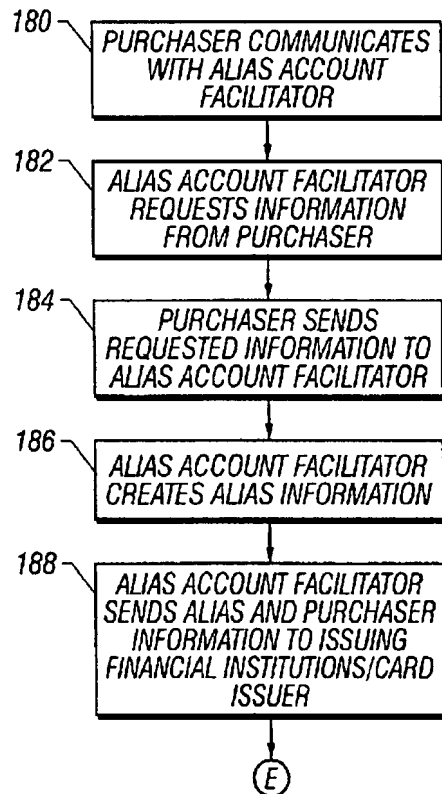


FIG. 6B

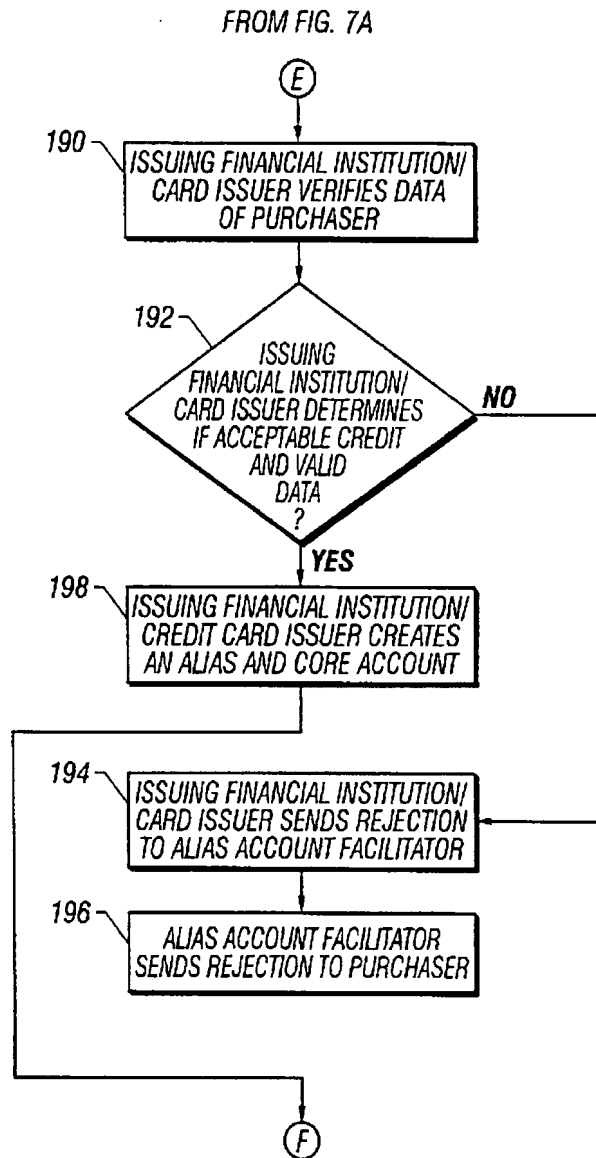
10/15



TO FIG. 7B

FIG. 7A

11/15



TO FIG. 7C

FIG. 7B

12/15

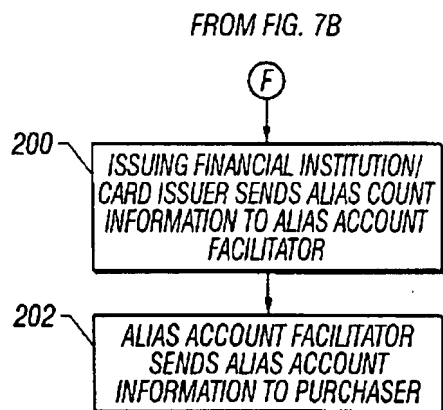


FIG. 7C

13/15

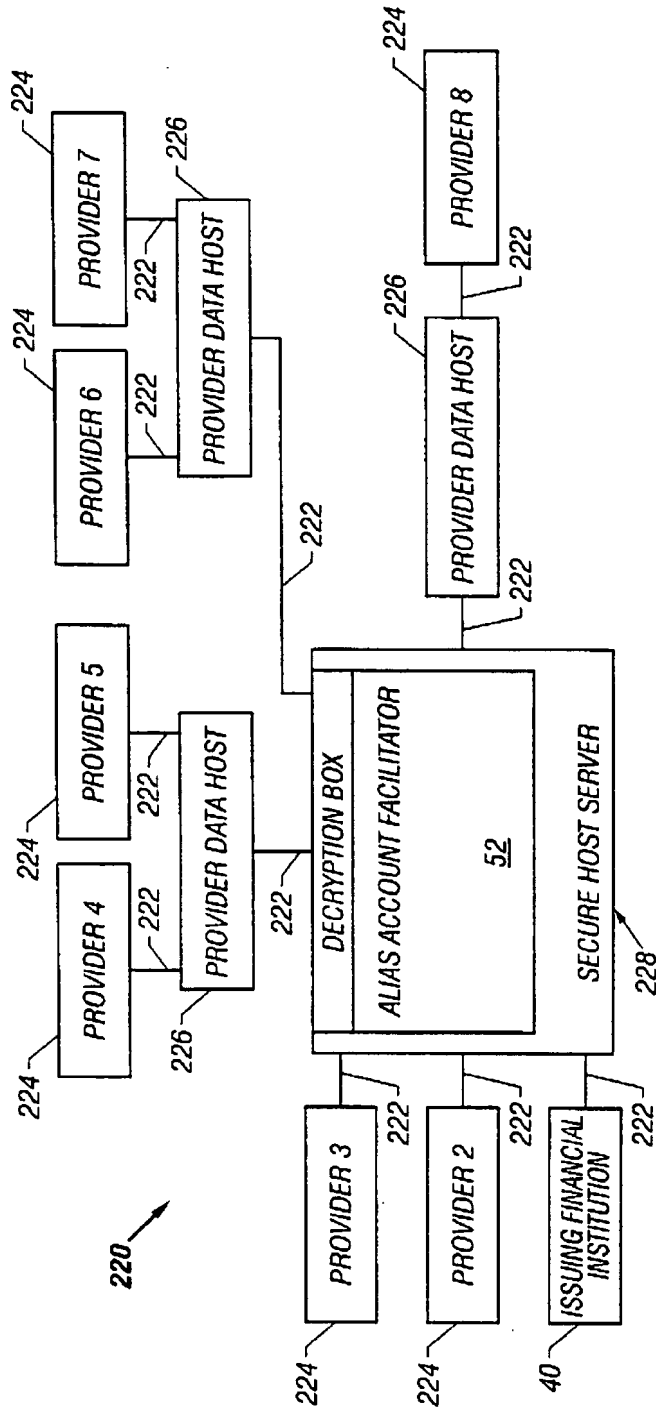


FIG. 8

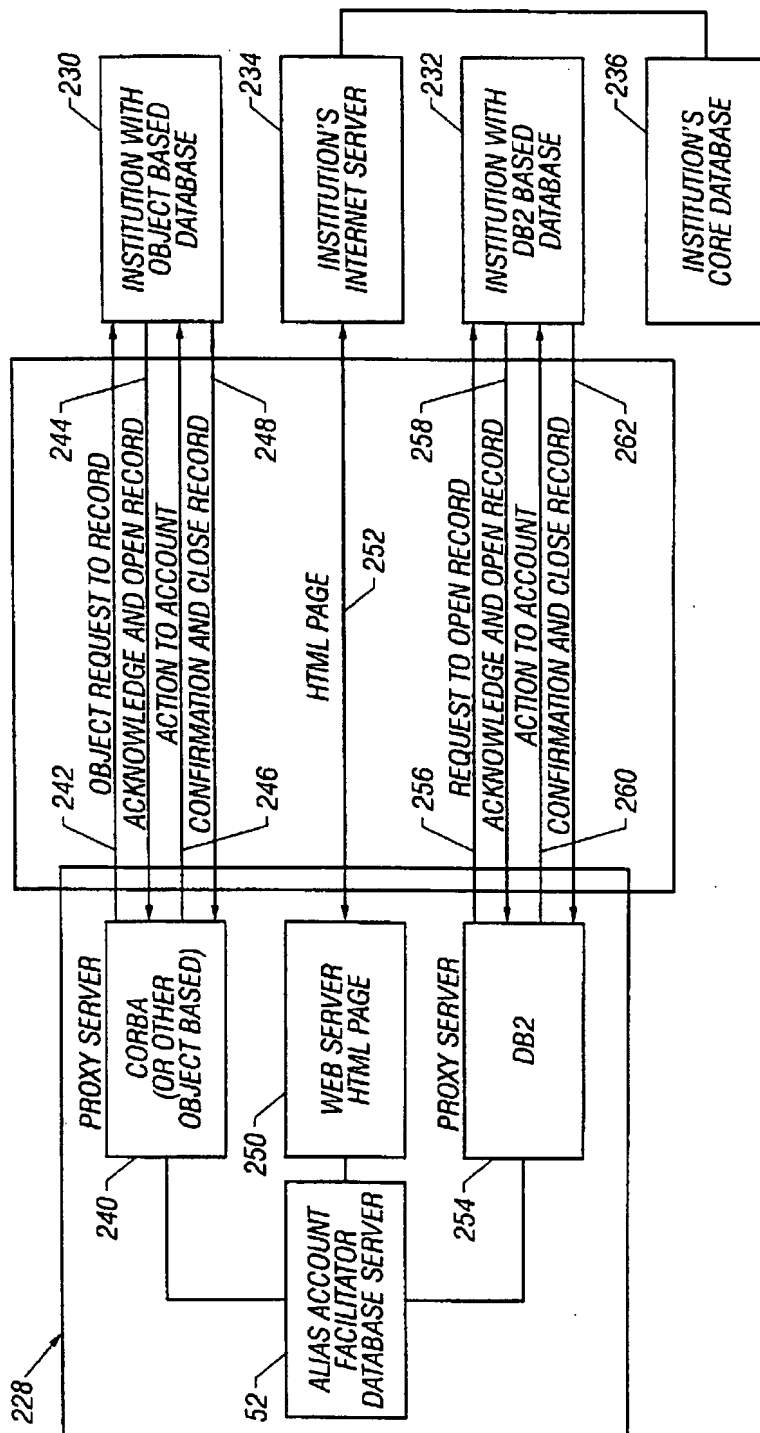


FIG. 9

15/15

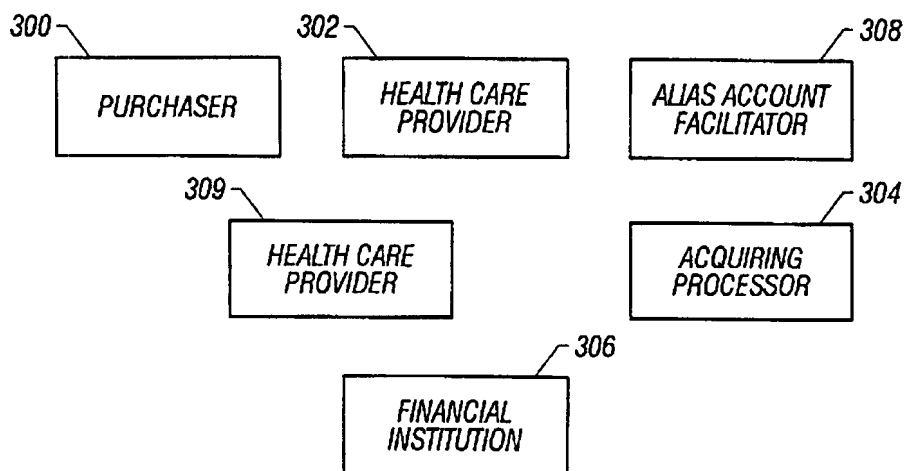


FIG. 10

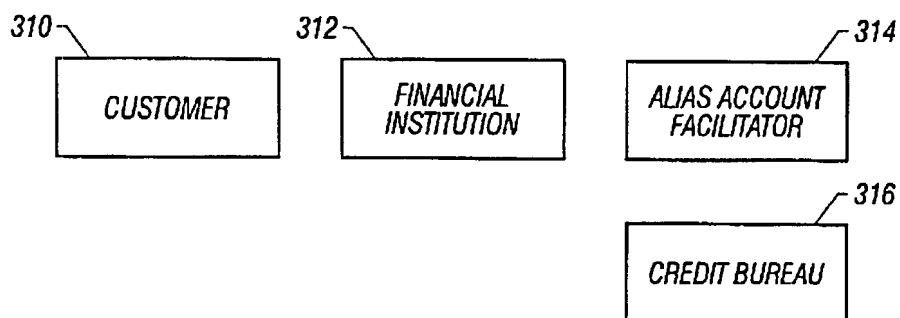
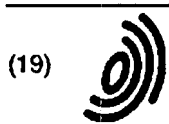


FIG. 11

*** Slip Sheet ***



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 917 119 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
19.05.1999 Bulletin 1999/20

(51) Int. Cl.⁶: G07F 19/00, G06F 17/60

(21) Application number: 98203747.5

(22) Date of filing: 09.11.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 12.11.1997 US 65291 P
14.04.1998 US 81748 P

(71) Applicant:
Citicorp Development Center, Inc.
Los Angeles, California 90066 (US)

(72) Inventors:
• Paltenghe, Cris T.
Northridge, California 91326 (US)
• Takata, Melvin Michio
Thousand Oaks, California 91360 (US)
• Mamdani, Alnoor Bahdur
Venice, California 90291 (US)
• Huddleston, Gregory Lee
Huntington Beach, California 92649 (US)

(74) Representative: Hynell, Magnus
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) **Distributed network based electronic wallet**

(57) A system, in which information is the primary asset and in which investments may be made in information, includes multiple data stores for storing different types of a user's information. The safe, secure and properly authorized transfer of information while preserving individual privacy is provided. The system also provides for secure backup and storage, as well as for ubiquitous and nomadic access to information while maintaining the privacy of such information. A first data store includes static identification data about a user. A

second data store includes moderately dynamic personal data about the user. A third data store includes dynamic demographic information data about the user. An electronic wallet can be used with the system to download selected portions of the data for use by the user. A method of use of the data includes using the data for billing out forms, providing services to the user and allowing merchants to selectively target users for sales while maintaining user anonymity.

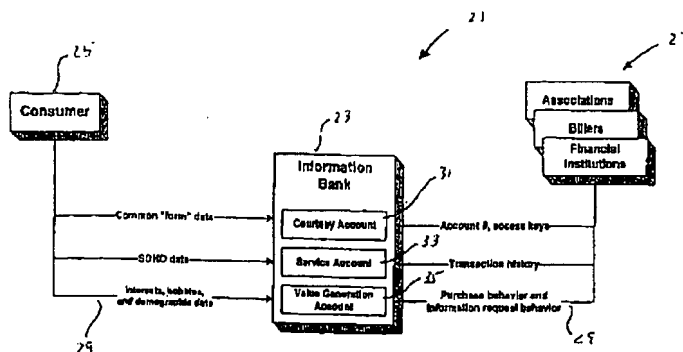


FIG. 1

EP 0 917 119 A2

Description

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to Provisional Patent Application No. 60/065,291 entitled "Distributed Network Based Electronic Wallet," filed on November 12, 1997, to which priority is claimed.

FIELD OF INVENTION

[0002] This invention relates to information storage and retrieval systems, and more particularly, to an electronic system for storage and authorized distribution of personal information.

BACKGROUND OF INVENTION

[0003] In today's information-based economy, information is recognized by many corporations as a primary asset which, much like currency, fully realizes its value only with frequent use. Information is an important asset not only for corporations, but also for individuals who often need to repetitively provide certain personal facts to merchants and service providers with whom they do business.

[0004] Collections of personal information, in the form of demographics, are invaluable to companies wishing to conduct targeted marketing campaigns. Examples of information collections include insurance policies, legal documents, medical records, and financial and credit histories. This information represents a valuable commodity which many corporations are willing to purchase.

[0005] In fact, many companies are known to massage their consumer accounts to create mailing lists which can be sold. Likewise, most consumers know this happens, and are not surprised to receive a barrage of catalogs from previously unknown vendors after placing a mail order for goods. Many consumers are annoyed by this practice and some may even avoid the offending vendor in the future in order to prevent further abuse of their personal information. However, most of these consumer concerns could be eliminated, or at least reduced, if this data were first scrubbed or sanitized to remove all references to the particular individual before being made available as marketing data.

[0006] Privacy is a growing concern in the internet and electronic commerce arena because each time you enter a site, your browser already tells the server a lot about you, such as which browser you're using and your IP address. This makes it easy for data miners to track site visits and strip information from unsecured data transmissions. In response, the Internet business community is promoting Open Profiling Standards (OPS) which allow individuals to save personal information on a hard drive on their PC and only allow others to access portions of this information after the individual grants permission.

[0007] There is also concern over the use of cookies, or tokens that are attached to a user program and change depending on the web site areas entered. When you enter a web site using cookies, you may be asked to fill out a form providing information such as your name and interests. This information is packaged into a cookie and sent to your web browser which stores it for later use. The next time you go to the same web site, your browser will send the cookie to the web server. The server can use this information to present you with custom web pages. Cookies are typically designed to be persistent and remain in the browser for long periods of time, and can be used to unknowingly disclose the address of the site you most recently visited, or movements within a site.

[0008] Consumers also increasingly want to systematically organize and secure personal information but are generally limited in their ability to do so by the availability of commercial software programs. For example, certain financial planning and management software packages provide a facility for storage of personal information on the consumer's PC. This practice can be vexing if the PC subsequently experiences an anomalous operation or a system malfunction. There is then a need for a system which would allow personal information to be professionally backed-up, thus protecting against mishap, natural disaster, negligence, or even PC theft.

[0009] Consumers also want the ability to control and define access to their information, using presently available technology to securely and privately store, sort and/or exchange information. There is then a need for a third party who would provide these types of services with a primary aim of preserving its consumers' personal privacy.

SUMMARY OF THE INVENTION

[0010] In one aspect the invention provides a system for the selective organization, access to and use of personal data. The system may include a server having data storage capability for storing different types of personal data in distinct data stores, i.e., an "information bank", such that the information may be efficiently used by the consumer and by institutions which the consumer has authorized to access the data. A first data store may include what is known as static identification data which is personal to a user such as a consumer and which is typically necessary for establishing a relationship between the consumer and an institution. Such a consumer will have a means to access the static identification data, such as a personal computer, network computer, smart telephone or other communication device through the Internet or other network connection or wireless connection. A second data store may include what is known as moderately dynamic personal data about a user or may users, again a consumer or consumers. This would typically include a large volume of data which may be difficult to manage and which is

stored primarily for the convenience of the consumer. A third data store may include dynamic demographic information data about the users or consumers. This data may be mined from the data stores mentioned above, or may be the result of information provided by the consumer, for example, in response to surveys. Typically, this information is valuable to many research and marketing institutions which may directly or indirectly compensate the consumer for access to the information.

[0011] For purposes of the disclosure herein, by the term "static identification data" is intended to mean a relatively small amount of data which is relatively static and which is typically necessary for establishing a relationship between the consumer and an institution. This type of data is stored for a indefinite period of time, typically at no cost to the customer. Examples of this type of data include name, address, phone number, social security number and other commonly asked for information on forms, applications, etc. This type of data can be used in services provided by an institution such as a bank as a free account to permit activities such as automated form filling, safe shopping and general electronic commerce. Such an account file can generally be referred to as a "courtesy account."

[0012] With respect to "moderately dynamic personal data", this is intended to mean a large amount of data, which is dynamic and which is stored over long periods of time. Such types of data includes, for example, billing history, payment history, loans, real estate holdings, stock, bond, fund holdings, medical records, home web pages and the like. This type of data can be used in services provided by an institution such as a bank on a charge for service basis, and may be used in the account for bill presentment/payment, relationship management, tax preparation, divergency information (medical records) focal point, and the like. Such an account and file can generally be referred to as a "service account."

[0013] As to "dynamic demographic information data", it is characterized by being demographic data including, user interests, user profiles and user agents. Examples include age, geographic location, race, religion, professional interests, hobby interests, frequent purchase categories, explicit requests for information, explicit requests for blocking categories of information. Customers who allow use and transmission of this data to others such as merchants could be paid a portion of receipts of selling that data received by an institution such as bank. The data can be provided to market research organizations, electronic census providers, organizations which provide profile special offers and the like. Such an account and file can generally be referred to as a "value generation account."

[0014] More specifically, a consumer's financial institution, by the nature of the transactions in which it engages, already has in its possession large amounts of confidential and disclosure-sensitive information. As

may be appreciated from the prior description, examples of this type of information include credit card purchases, income data, bank card transactions, loan application/servicing, etc. Thus, it is optimal for the financial institution to maintain principal possession, maintenance and storage of the types of information described previously for consumer authorized use and distribution, while simultaneously achieving, without the introduction of yet another party, the securing of the consumer's personal information in an "information bank."

[0015] In accordance with the invention, the consumer's information may be made available through the financial institution's computer network server, thereby allowing convenient "universal" access to the consumer's personal information, i.e., "static identification data". Thus, access to the consumer's information is only limited by access to standardized devices on computer networks, such as personal computers, i.e., PC's, network computers, PDAs, smart telephones and other communications devices which are connected to the financial institution through the Internet or other network connection. More importantly, the present invention eliminates the need for consumers to have direct access to the consumer's own PC, while at the same time providing required security and access authorization controls.

[0016] As noted previously, there is also a need to organize and utilize a much broader range of information, including personal information. This type of information further includes data that is commonly associated with an individual, i.e., the "moderately dynamic personal information", and can be accessed by specific types of organizations or entities such as doctors, tax preparers, etc. Essentially, this information is automatically transferred, upon consumer authorization, to another party in a format that can be used.

[0017] Finally, it is also desirable to organize demographic information, i.e., "dynamic demographic information data", from consumers into collections of data for evaluation and use by other institutions and individuals. May of these institutions and individuals, which include merchants and others engaged in commerce and institutions engaged in research, are willing to pay for access to such information. However, due to privacy concerns it is desirable to make demographic information available without disclosing sensitive information about individual consumers, such as actual name, physical address, e-mail address, telephone number, etc. to a institution. Therefore an inquiring institution, for example a merchant, can come to the institution storing the consumer's data, such as a consumer's financial institution, and request an information-based (e.g., electronic) profile of the kind of consumer to which its products and services would be suited. Such a profile would typically include the number of consumers within the database that met certain criteria. The merchant could then request that the financial institution deliver information

or advertisements of its products or services to individuals which meet certain criteria. The financial institution would then deliver the information or advertisement to individual consumers thus preventing direct contact between the merchant and the individual. After the consumer has the opportunity to anonymously review such information, the consumer at its own discretion may choose to contact the merchant.

[0018] A portion of the fee charged by the consumer's financial institution for the request and receipt of the consumer information may be used to pay the consumer as an inducement to participate in the transaction. Accordingly, the consumer is investing information for financial and/or non-financial gain. One example of non-financial gain might be the receipt of loyalty credits, as in the case of airline mileage points. Therefore, the consumer is remunerated by the financial institution depending on what the business strategy requires.

[0019] The system of the information bank can thus provide, in specific aspects, three types of accounts: a courtesy account, a service account, and a value generation account. Basic information can be stored in the information bank courtesy account and used for automated "form filling" services which are useful to the consumer as an easy means for providing personal information to others when and as authorized. This service may also include a digital signing service, a digital signature verification service, and, for example, notary services.

[0020] The information bank system's service account is appropriate for larger amounts of consumer generated data which grows steadily over time. The service will provide for secure backup and storage, as well as for "ubiquitous" and "nomadic" access. Service accounts may hold transaction logs, account histories, medical records, insurance information, financial records, etc.

[0021] As personal computing devices become more accessible and "connected" through the Internet and other home networks, the requirement for home data storage devices may decrease. Since "standard" consumer software applications such as e-mail and home accounting packages have become readily available across distributed commercial networks, there is now a corresponding need for network based information storage and safekeeping such as is provided in accordance with the invention. One advantage of using networked information storage is that consumers will have access from many locations, and will not have to carry the information with them when they travel, as do people today. The consumer's information can be made securely and privately available, for example, through "set top boxes" i.e., cable system boxes used on television, and having advanced architecture such as RISC based technology, in hotel rooms or on terminals in emergency hospitals upon authorized demand via smart cards or other similar devices.

[0022] The service account will also provide software

and data backup/archival services for small office/ home office (SOHO) proprietors who prefer not to own standard office software applications, and who wish to know that their business records and data are securely and professionally managed.

[0023] Another feature of the service account is to provide third party access to otherwise confidential information in the event of accident, emergency, or death. For example, an unconscious accident victim can't provide PIN or biometric access to urgently required medical information. Under these or other appropriate circumstances, the service makes stored medical information such as patient allergies, medications, medical history, etc., available to authorized recipients. This feature also allows estate executors to access information that is required to handle estate matters, for example, private keys.

[0024] Storing data in a self describing meta language, such as XML format, facilitates transfer and use of data by third parties. With proper account owner access authorization, the service facilitates access and understanding of stored personal information, which should reduce the dollar and time cost of services provided by third party professional service providers, such as accountants or physicians.

[0025] The service account may also include a cryptographic key escrow and recovery service which provides key escrow and recovery service by storing a key pair and certificate copy after these are generated by a browser, or by generating a key pair and certificate and storing a copy. The service then provides a replacement copy of the key pair and certificate in response to an authorized consumer request.

[0026] The present invention will enable the establishment of a trusted third party service to market demographic and other valuable marketing type information to manufacturers, distributors, and other marketing concerns, while protecting an individual's identity. Fuzzy logic matching is used to match merchant and consumer, on an anonymous basis so that neither knows the identity of the other, and allow consumers to search, shop, and negotiate anonymously, with only items that match their interests being brought to their attention by the service.

[0027] The system information bank may also serve as clearing house and mint for value exchange units created for use as coupons, tickets, tokens and other loyalty schemes. All of units will go through essentially the same creating, capture, redemption, and automated clearing functions. The information bank can provide services related to the creation and maintenance of loyalty programs. These coupons, tokens, etc. can be stored in the information bank and temporarily distributed to or tracked by, for example, an electronic wallet. For purposes of this disclosure an "electronic wallet" is a virtual container for the various information and financial application a user might want to be mobile. The information is generic in nature, and the "wallet" can be

made to hold a heterogeneous collection of applications that are not necessarily affiliated, or even offered by the issuer of the wallet. The applications can be added "ad hoc" after issuance of the wallet. Although not required, one example of an implementation of the "wallet" is through the use of "smart card" technology of the type well known to those of ordinary skill in the art.

[0028] The system of the information bank also provides the ability for consumers to specify certain important events of which they wish to be reminded or notified. The consumer can also define a notification hierarchy or priority, e.g. cell phone, work number, e-mail, home number, etc. and the tenacity built into the system for notification for each event.

[0029] The "information bank" also includes the ability to provide an anonymous shopping service which allows the shopper to span multiple merchant sites and shopping services. The information bank intermediates the consumer shopping by assigning the consumer a different alias for each site in order to make cross correlation by data scavengers more difficult. Orders to popular merchants are consolidated and paid in a lump sum. Consumers are billed internally by the information bank, so no consumer payment identification information crosses the Internet or is made available to merchants. Consumers may have goods shipped to a drop address from which a third party re-ships the goods to the consumer so that the merchant never knows the identity of the consumer, and the re-shipper does not know shipment contents.

[0030] The service also provides Internet and point of sale identity protection. By substituting the consumer account name with a random number every time the user's information is sent over the network, the information bank keeps track of the aliases it generates and internally routes responses to appropriate parties while preserving anonymity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] Having briefly described the invention, it will become better understood from the following detailed discussion, viewed with reference to the attached drawings, wherein:

FIG. 1 presents a general overview of an embodiment of the present invention;

FIG. 2 presents a general overview of a use of a first specific data store as implemented in the system;

FIG. 3 presents a general overview of a use of a second specific data store as implemented in the system;

FIG. 4 presents another general overview of a use of a second specific data store as implemented in the system;

FIG. 5 presents a general overview of how a consumer inputs information or data into the second

specific data store of FIGS. 3 or 4;

FIGS. 6 and 7 present a general overview of alternative ways of how consumers may access the second specific data store, i.e., the service account, in the system;

FIG. 8 is a detailed overview of the use of a third specific data store as implemented in the system, in combination with the use of the first and second specific data stores;

FIG. 9 is an alternate overview of the use of a third specific data store as implemented in the system;

FIG. 10 is an overview of how certain events trigger notification to consumers using the system;

FIG. 11 shows how the system may be implemented to provide consumer information to merchants on an anonymous basis;

FIG. 12 is a table showing the different types of data in the different accounts of the system;

FIG. 13 is an architectural overview of an electronic wallet to be used in the system; and

FIG. 14 illustrates a wallet and application access scheme.

DETAILED DESCRIPTION

[0032] The information banking system which includes a distributed network based electronic wallet provides a means for consumers to interface with both the information bank and third-party providers of goods, services or information who are referred to herein as merchants. In Figure 1, the consumer 25 is shown either interfacing with an information bank 23 and various merchants or service providers 27. This can be done by the consumer 25 through a home PC or at a walk-up kiosk type device which utilizes smart card technology. Connection to the information bank 23 can be through conventional transmission lines 29 such as telephone lines, cable, wireless communication, etc. Regardless of the type of user interface chosen, the consumer communicates through the network 29, to the information bank 23 and/or the merchants or service provider 27. The network may be a closed network, accessible only to the consumer 25, the information bank 23 and approved merchants or providers 27, or it may be a network such as the Internet, where all transactions are conducted in a secure manner well known in the art through appropriate encryption. The information bank 23 can be made up of a conventional server with appropriate data storage. Within the data storage, separate files or accounts can be defined as will be readily apparent to those of ordinary skill in the art. Communications between the server and other users/devices is achieved by conventional means such as a telephone modem, cable modem or other like established and well known systems.

[0033] In Figure 1 there is shown an overview of the types of accounts which will be maintained at the information bank 23 and the types of information retrieval

which the consumer 25 can control. The consumer's authorized information will be either requested by or relayed to various merchants or service providers 27 consisting of associations, billers, or financial institutions with whom the consumer 25 wishes to transact business. One type of consumer account is known as a courtesy account 31 and holds certain home or personal information, such as the name, address, phone numbers, e-mail address, birthday, social security number, mother's maiden name, spouse's information and other familial information which is commonly needed to fill out forms or otherwise identify the consumer to those with whom they do business. This type of data is typically known however as "static identification data" as has been described and will become clearer further herein.

[0034] A second type of account is a service account 33 which is maintained for the benefit of the consumer and contains "moderately dynamic personal data" about the consumer 25, as well as software programs which can be accessed by the consumer 25, and which may be accessed or populated by various merchants or service providers 27 as authorized by the consumer 25. For example, banking accounts, insurance information, tax returns, and other consumer data can be stored in the service account. This data is characterized by being a large amount of data which is dynamic and stored over long periods of time. It can be used for functions such as bill presentment/payment, relationship management, tax preparation, and other purposes as will become clearer further herein.

[0035] Figure 1 also shows a third type of data known as "dynamic demographic information data" which is kept in a value generation account 25. This file or account 35 is provided as a means for the consumer 25 to define certain demographic data, including a generic consumer profile, interests and hobbies, and the types of information the consumer would like to receive from third parties. This information is stored in the value generation account 35. Upon request by a third party merchant or service provider 27, a profile or aggregate of consumer information may be provided to the third party merchant or service provider by the information bank 23 for a fee. The profile or aggregate of information about participating consumers will not provide information which identifies individual participating consumers, but will rather provide the third party merchant or service provider with sufficient information to determine if it will request that the information bank provide consumers with advertisements of its merchandise or services. Merchants or service providers 27 will likely agree to pay for this aggregate consumer data and for indirect access to the consumers whose information is contained in the data bank because it will enable the merchant or service provider 27 to direct specific offers to a targeted market in an efficient manner.

[0036] Figure 2 illustrates, one example, of how the courtesy account can be used as a form filling service.

In this figure, there is a three-way relationship between the merchant, in this case a doctor 39, the consumer 25 and the information bank 23. First, the merchant, or in this case, a doctor 35 will send a permission request for information to the consumer 25 through a separate connection 37 which can be the Internet, a dedicated line, a phone call, etc. The consumer 25 will then send a permission message, including a verifiable signatures, back to the doctor 39. The doctor 39 will then forward an information request through, for example, use of communication device, including a now verifiable permission to the information bank 23. The information bank 23 will verify the permission as being valid for this particular consumer 25 before forwarding the consumer's personal information to the doctor's office 39. The information in this scenario is originally entered by the consumer 25 directly into the information bank 23. It is also expected that a merchant or a service provider, such as a doctor, who maintains information about an individual, such as a history of immunizations, could have such information directly transmitted to the information bank when the doctor is authorized to do so by his patient. This would give the patient/consumer the convenience of having the merchant or service provider provide the Information Bank with a medical history or with update information, such as a recent immunization, about the patient/consumer without the inconvenience of the patient/consumer having to manually forward such information to the Information Bank which would then have to take the additional step of entering the data. This would also save the doctor the cost of storing the records.

[0037] Of course, this type of service is not limited to form filling. In a more general sense, the Information Bank allows the consumer to grant conditional, single access or limited access to service providers or merchants such as tax specialists, loan brokers, financial planners, and similar entities, which typically use information provided by a consumer. After retrieving the consumer's information, these entities may generate compilations and/or analysis of the consumer's data and, for example, prepare a tax return, loan application or financial plan for the consumer. The service provider could then either return the prepared document to the consumer or directly file documents such as a tax returns if authorized to do so by the consumer. Resulting information might also be incorporated into the consumer's information stored in the Information Bank for future access and/or analysis.

[0038] Figure 3 depicts the use of the information bank service account 33 to provide a signing service. Such a service may be provided where a consumer 25 requests such a service and provides the service institution with adequate authorization, such as a power to attorney, to provide signatures for the consumer. As shown in this diagram, the consumer 25 forwards an unsigned document to the information bank 33 where cryptographic software 39 which is conventional in

nature and well known to those of ordinary skill will be used to authenticate the consumer 25 and generate a signed document for return to the consumer 25. Also, it is expected that the consumer may authorize the information bank to sign certain documents for the consumer which have been transmitted to the bank by third parties. In such a case, the consumer would review the document and instruct the information bank to sign the document. The information bank could then return the document to the consumer or to the third party if requested by the consumer.

[0039] Electronic commerce requires certain trust components be implemented for signing services. More specifically, current digital signing procedures require parties in electronic transactions to provide critical trust components such as encryption and non-repudiation services. The current public key infrastructure (PKI) which is promoted by various vendors involves certificate authorities (CAs). For the power of attorney signature service described above, the information bank would provide the required key and certificate authority without requiring access to any private verification information or key possessed by a consumer, but would instead provide all authentication services through the information bank service. The information bank would in turn require adequate authentication from the individual consumer for execution of the signing service.

[0040] By implementing a digital signing service with appropriate software 39, the information bank 23 can be used to remedy or eliminate many of the issues related to registration, certificate issuance, certificate verification and certificate revocation lists (CRLs). This also reduces the size of the data transfer required for a verified transaction, because a standard certificate includes the certificate holder's identity, the certificate serial number, a certificate holder's expiration dates, a copy of the certificate holder's public key, the identity of the CA, and the CA's digital signature which is used to confirm that the digital certificate was issued by a valid agency.

[0041] The present invention also provides for digital signature verification and notary services. This is illustrated in Figure 4. Current PKI solutions require several components in order to verify the integrity of a digital signature. Besides the document and the signature itself, all certificates in the chain to a trusted root and access to the CRLs for each CA must be available. These components are then fed into a software program that verifies first, that no certificate was on a CRL at the time of signature; second, the integrity of each certificate in the chain based on the public key of the next higher certificate in the chain is unquestioned; and third, the integrity of the original document. A consumer 25 wishing to perform this process needs access to this software, but they must also trust the software that's performing these checks. That is, if the software provides a valid or invalid signature result, but the software is not adequately safeguarded on the consumer's machine, then any result provided by this software is

suspect.

[0042] The signature verification function offered by the present invention provides a simplified and trusted method for verifying the integrity of additional signatures. A consumer 25 is not required to understand the intricacies of CRLs and is not forced to load cryptographic software onto his access device. Instead, the consumer 25 just forwards the signature and request to the information bank 23, which performs the appropriate checks. In this case, the cryptographic software 39 is already loaded into the information bank 23, but the CRL and root certificate are provided through line 41 to the information bank 23 to perform the verification for the consumer 25. An alternate function, somewhat related to signature verification, is an actual signing function. In providing a signing function, the information bank 23 accepts an unsigned document and signs it on behalf of the consumer 25. Another benefit of offloading the signing and verification process to the information bank 23 is that it reduces the overhead on the consumer 25 device. It takes quite some time to generate a 1024-bit key pair using a browser on a current Pentium processor. The information bank 23, however, will be running this software on a state-of-the-art machine as previously discussed, which is capable of quickly performing this function. Furthermore, the information bank 23 will operate in a secured environment which will eliminate any questions related to software integrity, and will provide access to all required CRLs and route certificates from the appropriate X.500 directory structures through connections 41, many of which are likely to be stored in local cache memory. The information bank 23 also functions as a secured backup and storage facility service.

[0043] As more and more consumers begin to use electronic commerce and related electronic bill paying services, consumers will need to maintain important home records related to these transactions on their own PCs. The consumer may soon have access to and require safe storage for electronic copies of insurance policies and other legal documents. Many consumers already create large amounts of data with personal financial software, such as those commercially available under the names Quicken or Turbo Tax. The secured backup and storage service provided by the information bank 33 provides the consumer 25 with the capability to safely and securely store important documents on servers which are professionally managed and reside on Information bank 23 hardware. Storage remote from the consumers' PC provides a disaster recovery plan and mitigates any problems associated with hard disc crashes, fire or theft.

[0044] Figure 5 provides an overview diagram of the types of personal financial information which will be resident on or managed by the information bank's secured backup and storage devices. Personal financial information, such as banking, bill presentment, stocks, mutual funds, 401K accounts or IRAs, all collectively identified

with the number 43, can be transferred to the information bank through connections 29 under the consumer's control. Legal documents such as insurance policies, wills, deeds, contracts and other electronic commerce documents can also be forwarded to the information bank 23 for secure archival. Electronic artifacts, such as coupons, point of sale receipts, tickets, tokens and other forms of loyalty credits can be made by the consumer 25 and tracked in the information bank 23 in a secured manner. Important medical records will increasingly be created and stored electronically by medical service providers, and such records of consumers' allergies, medications, past x-rays, diagnoses and doctor's notes can be stored by the consumer 25 and securely and confidentially saved at the information bank 23 in the service account 33 for release only as approved by the consumer 25. In the preferred embodiment the consumer 25 would instruct the third party merchant to forward this information directly to the information bank 23 and it would then be stored therein for the consumer. In an alternate embodiment, these financial and personal documents would be moved from the third party merchant to the consumer 25 and then forwarded by the consumer to the information bank 33..

[0045] Another office related service is the virtual office provided by the information bank 23. This service compliments the storage and secure backup by, for example, providing software for students, or for use at small offices or home offices. Suites of office software, including word processing or spreadsheet programs, could be provided for the cost conscious individual who has Internet access but does not necessarily have the resources to pay for, or the desire to continually update and manage, a home office software library. This can be provided by the service account 33 and implemented in a conventional manner well known to those of ordinary skill in the art. Subscribers to this service would be able to execute the software when needed and would never have to worry about upgrades or system compatibility, which would be managed by the information bank 33 which transmits the software to the consumer 25 for use by the consumer 25 on the consumer's device, e.g., home computer.

[0046] The information bank 23 can be used to coordinate the consumer 25 information stored in the information bank 23 with third party service providers in order to more conveniently allow the consumer 25 to use the third party services. For example, the information bank 23 may be used to provide software which will facilitate the downloading of certain consumer information to printing services or in case of emergency, to medical providers. The information bank 23 may also be programmed to release this information to, for example, executors of the consumer's estate if previously authorized to do so by the consumer 25. By being able to share information generated by various service providers, the consumer 25 will find that many previously burdensome tasks are now easily accomplished. In the

preferred embodiment, this data will be stored in a self-describing format, such as the XML protocol for easy transfer to and use by various third parties.

[0047] Both Netscape and Microsoft Corporations market web browsers which currently provide support for generating key pairs. However, if a user is so unfortunate as to suffer a disc crash or has failed to update the browser software, it is possible that a user could lose the keys forever. Once this happens, there is no way to retrieve the information previously encrypted with the keys. The information bank 23 may offer a key escrow and recovery function as further depicted in Figure 6 to protect the consumer 25 against catastrophic key losses. In Figure 6 the consumer 25 uses software, such as a browser, which can generate a key pair generation request and forward it to the information bank 23. The information bank 23 then generates a key pair and certificate, saves the key pair and certificate, and forwards them to the consumer 25 for use. A second option is shown in Figure 7 in which the consumer 25 using browser software, generates the key pair and certificate and then forwards the key pair and certificate to the information bank 23 for archival. If the consumer 25 ever loses a key pair, the consumer 25 can request and receive a replacement copy from the information bank 23. To accomplish all of this, of course, cryptographic software 39 is required, the details of which will be readily apparent to those of ordinary skill in the art.

[0048] The information bank 23 is configured to generally facilitate electronic transactions and make the consumer's life easier and more convenient. The value generation account 35 to be discussed in greater detail hereafter, can be used to provide assisted product, service, or information searches which not only make consumers' lives more convenient, but also provide consumers with some value in return for using the service. This value may be in the form of monetary compensation or it may be in the form of loyalty credits with preferred merchants selected by the consumer 25. This is an optional service and is completely controlled by the consumer 25. The consumer 25 can make their hobbies, personal interest and demographic information available, while keeping their identity private. A consumer profile is compiled by the information bank 23 from both explicit and implicit information. The consumer 25 is given full control and can specify constraints on information and specifically exclude certain information from product, service, or information search categories. Merchant offers which satisfy the consumer criteria are forwarded by the information bank 23 to the consumer 25. In this system, the merchant will not know the identity or address information of the consumer 25, nor will the consumer 25 know who the identity of the merchant. The information provided must be presented with a summary demonstrating how it satisfies the original interest of the consumer 25 and may include short promotional information. The consumer 25 has the opportunity to request more information or request a

purchase. Up to this point, the advertising provided from the merchant to the consumer 25 has been free to the merchant. This allows the merchant to get real time demand statistics and other valuable aggregate indicators of the quality of their offer free of charge. However, in order to complete the final transaction, a fee is required for the merchant to continue. In this way, these advertising dollars are spent by the merchant, knowing they are highly correlated to a targeted sales market.

[0049] Figure 8 illustrates such a process where the consumer information from the consumer 25 device is entered into the information bank value generation account (previously numeral 35 in FIG. 1) in the form of a profile. In this case, the information bank 23 is shown as consisting of an information bank portion 123 consisting of the courtesy account and service account previously discussed. The information bank 23 will also include the value generation account module, i.e., number 125 herein, an independent consumer advice module 127, a transaction module 129 providing, matching, brokering, consolidation and accounting functions, and a merchant gateway module 131 which connects to the merchant 133. In this embodiment, the value generation account module 125 takes input from the courtesy and service accounts 123 in the form of explicit and implicit (mined) data. The consumer 25 profile is updated from this data and is provided to a module 129 having a matching function running in the information bank 23. The matching function also is connected to receive offers from a merchant gateway module 131 which is connected to the merchant 133. Merchant offers which sufficiently match the consumer 25 profiles will be forwarded by the information bank 23 to the consumer by the module 129 for review. When a consumer 25 indicates interest in a particular offer, they will issue a request or a buy request back to an information bank consolidator function in module 129, which will then forward this to the merchant 133, either individually or in bulk with other consumer offers. The merchant 133 will then pay a fee for the brokerage service and portions of this will be split by the information bank 23 and allocated to particular consumer accounts as appropriate. This function also includes an independent consumer advisor module 127 which includes data available to the consumer 25 for reference, and provides background information about various merchant offers.

[0050] The fees paid by a merchant for access to the consumer information could also be structured such that the fee would increase based upon the type of usage by the merchant. For example, a certain fee could be assessed for access to view a customer information summary. The fee would then be increased if the merchant chose to request that information be provided to individual consumers. A further fee increase might be levied if a consumer chose to respond or purchase a merchants product after being solicited through the information bank. Other tiers of services and fees are

also contemplated.

[0051] The information bank 23 may also be programmed to provide, for example, a coupon, ticket, token and loyalty management program in which the information bank 23 serves as a mint and clearinghouse for units created for use as coupons, tokens, tickets and other loyalty schemes. Although exhibiting a wide variety of outward appearances, the internals of the minting, capture redemption and automatic clearing functions would work essentially the same. This function is valuable to the consumer 25 because of added functionality in an electronic wallet (to be described hereafter) to keep track of various coupons, tokens and ticket acquired by the consumer.

[0052] A coupon and loyalty management program is depicted in Figure 9 as including several components of the information bank 23. These components include a clearinghouse module 139, a retailer gateway Module 137, a service account Module 123, credit exchange module 135, a manufacturer gateway Module 141, and interfaces to merchants who can be either retailers 147, manufacturers 145 or service providers, such as an opera house 149 or ticket issuer 143.

[0053] As further shown in Figure 9, the information bank manufacturer gateway module 144 can be programmed to mint a coupon and issue this via the manufacturer 145 electronically to the consumer 25 who will then store the coupon in the information bank service account 33 or in an electronic wallet therein. Coupons may be issued by manufacturer, distributors and/or retailers, and tickets may be issued, for example by various entertainment and/or educational concerns. Tokens are issued by a wide variety of concerns ranging from transportation authorities to entertainment establishment. Almost any retailer or business could create a loyalty program using tokens. The consumer 25 in receipt of a coupon, ticket or token would store these in a service account or smart card electronic wallet. When the consumer wished to redeem these coupons, they would forward them to the information bank retailer gateway module 137 which presents the coupons to the information bank clearinghouse module 139 for settlement. The information bank manufacturer gateway module 141 then would issue an appropriate credit back through the information bank clearinghouse module 139 to the appropriate retailer 147 in exchange for the redeemed coupon. All of these functions can be implemented routinely by those of ordinary skill in the art using existing hardware and software tools and devices once the broad functionality described in detail herein is known.

[0054] As shown in FIG. 10 the information bank can also provides an important event, notification and response function. Such a function serves to allow the consumer 25 to specify certain events that are important to the consumer 25. Such events could be birthdays, stock price movements, loan availability, extraordinary bill charges, personal information

requests, etc. The consumer 25 can establish a hierarchy for the information bank 23 to locate the consumer 25, such as trying the consumer cellular phone first, then a work number, then e-mail, then a home number. When an event occurs that matches a trigger, a event notification is generated by a monitor program 151. The priority of the event would determine the degree of tenacity the service asserts in order to notify and obtain notice of verification from the consumer 25. This process is shown in Figure 10, where the consumer 25 sets specific event triggers and stores these in the information bank service account 33. The information bank then constantly monitors the event notifications with the monitor program 151, and when there is a match for a trigger event, the information bank 23 provides notice back to the consumer 25, based on the notification hierarchy previously defined by the consumer.

[0055] The information bank also provide an anonymous shopping service. This service, as shown in Figure 11, allows several components of the information bank (such as the service account 33, an anonymizer module 153 which assigns an alias to all consumer transactions, an order payment consolidator module 155, a junk e-mail investigator module 157 and a reshipper module 159 to work together to provide a intermediate shopping service which allows the consumer to browse certain merchant displays over the Internet without revealing their identity. The modules and functions described are conventional and well known, for example, from such services already available from certain web service providers. However, to date, no one has integrated the noted functions and modules into a coherent functioning system as provided by the present invention.

[0056] The anonymous shopping feature is similar to the assisted product, service, and information search, but this feature assumes that the discovery and comparison work has already been done, either through merchant offers forwarded to the consumer, or by the consumer's independent investigation.

[0057] This feature is more like a "shopping cart" on a website or service provider site on the Internet, where the shopper can span multiple merchant sites and shopping sessions and create a consolidated order. The information bank 23 serves as an intermediary for the consumer 25. The identity of the consumer 25 is replaced by an alias that is remembered by the function for subsequent reference. A different alias can be used for each merchant site, making it difficult for data scavengers to cross-correlate consumer purchases based on the alias. Junk e-mail originating from unknown sites can be traced to the site selling the address information via the alias.

[0058] This function consolidates orders to popular merchants and pays these merchants directly in a lump sum, together with a summary of orders and corresponding ship-to addresses. The consumer 25 is billed internally so that their credit card and other identification

information is never exchanged over the Internet.

[0059] For an additional shipping fee, the consumer has the option of having goods shipped initially to a drop box or reshipper address where a third party will take the goods and reship them to the consumer 25 at his/her stored address. In this manner the merchants never know the address or identity of the consumer 25. The packages are handled anonymously and a reshipping services does not know package contents.

[0060] With respect to the types of data stored by the information bank 23, as previously discussed, in particular with the first data store which is stored on the data storage mean, which includes static identification data, the second data store stored on the data storage and which includes moderately dynamic personal data, and the third data store which includes dynamic demographic information data, this is more clearly illustrated in FIG. 12. The courtesy count as shown in FIG. 12 includes the static identification data which is personal to a use having access to the information bank 23. The second data store correspondences to the dynamic personal data in the service account, and includes data about the user such as billing history, payment history, etc. The third data is the demographic data and will be stored in the interest bearing account to generate remuneration for the consumer in exchange for allowing use of that data. All of the types of data described have been previously discussed and are further expanded and illustrated in the table shown in FIG. 12.

[0061] Turning now to the use of an "electronic wallet" as previously described for use in connection with the system 21 of the invention, such a typical wallet 171 is shown in FIG. 13 which shows a typical architecture for such a wallet 171. The concept of an electronic wallet means many things to many people. One version would be a pocket sized computer with a snap shot-size color screen that will be used in place of many essentials that consumers carry around with them today such as money, keys, identification, credit cards, tickets, as well as items that provide the consumer with mobile information and communications such as a watch, newspapers, calculator, portable telephone, pager, etc. In this embodiment, the wallet 171 is a physical thing that is carried in the pocket. Because of its electronic nature, it can add functionality that the conventional wallet can not perform. However, consumer concerns about this type of device make it impractical. Although it is technically possible to back up the contents of the electronic device, the reality is that consumers would probably be at least as irresponsible with such a device as they are currently with their own data. Further, to the extent that such a wallet interfaces with providers of the wallet or others, there is a security concern in that information about the consumer could be used by others to make a profit and not let the consumer know about it. Thus, extension of the physical wallet, especially those offered by third party software or hardware vendors make rapid adoption unlikely.

[0062] At the other end of the spectrum is the totally virtual wallet. It is not a physical device, but a set of applications on a server somewhere. The major disadvantage of this approach is that all transactions have to be "on-line" or connected to a server. This could result in more expensive and/or less convenient use. Another issue is security.

[0063] A hybrid approach, and that preferred in accordance with the system 21 of the invention, is to put some data and applications on a physical device and some on a server. A smart card is ideally suited for this type of application since it makes the most sense to put the security and access functions on the card, and to put the volume of data and applications on the server such as the information bank 23. Further, those transactions that would be too expensive to have on-line, such as small amounts of electronic cash transactions, also makes sense to have on a such a smart-card. Thus, as shown in FIG. 13, the electronic wallet 171 in one embodiment is made up of an e-cash applications container 173, an electronic cash application manager 175, a use or authentication module 177, a key to application manager 181, a key ring applications container 183, and external applications interoperability API (applications program interface) 179, and a user application organizer and manager 185.

[0064] The e-cash applications container 173, as the name implies, is storage for e-cash applications. In order to gain critical mass, more than one type of e-cash is supported. The storage in container 173 is sufficiently generic to only record each of its members as being some form of e-cash and the actual "object" in the container 173 is a "connector" to the real e-cash application. The programming provides that the e-cash application can be located and started. The e-cash manager 175 is software that provides how to add e-cash applications and use them in a generic manner. The user authentication module 177 can be replaceable to allow for growth in the security and authentication technologies. Prior to implementation of smart cards, it could be software that asks for an account number and personal identification number, but with current technology, it can be implemented using the card and a server, using authentication technology implemented today. For future purposes, alternative security and authentication technologies might use biometrics, etc.

[0065] The key to application manager 181 serves to manage non-cash applications in the wallet such as credit, debit, e-checks, identification, facilities access and other applications. This is the software that maintains the contents of the key ring application container 183. The key-ring container 183 holds the connectors to server applications. The contents are managed and maintained by the key to application manager 181 previously described. Even as smart cards become more commonly available, it is believed that they will not be sufficiently large to actually hold the applications. Instead, they will hold "connectors" to the applications

that reside on a server. The most important aspect of a "connector" is a key or certificate that helps identify an authorized user of the application. The "key ring" then is a container of keys. They are not like the "real" keys, however, as further illustrated by FIG. 14 hereof.

[0066] More specifically, FIG. 14 illustrates a wallet and application access scheme 201. In this figure, the concept of an access device provider, wallet issuer and application provider have all been separated. As illustrated in FIG. 14, the consumer 25 can use an access device 203 to access their information 205. The access device 203 has been provided at point of sale, or point of contact by some party. The wallet then uses the access device 203 and the access device server 207 connection to the network to contact the wallet issuer server 209. The consumer 25 then identifies the appropriate application by their own description. The description is associated to a application key proxy 211 that is sent to the application provider server 213.

[0067] In the scheme 201 described, the consumer 25 can access their information via a device 203 provided at point of sale, or point of contact by some party. Since this party will want some presence other than the device 203, some "real estate" is set aside in the presentation interface for their content. The wallet 171 uses the device 203 and the devices server 207 connection to the network 201 to contact the wallet issuer server 209. The consumer 25, as noted previously, identifies the appropriate application by their own description. The description is associated to an application key proxy 211 that is sent to an issuer server 209. The issuer server 209 authenticates the user 25 and then looks up the location of the application and its real and actual key to be used for access to it. It then connects the consumer 25 to the application at the application server 213 and serves as a secure conduit.

[0068] As may be appreciated, proxies are used instead of actual keys in case the card is lost or stolen. In this manner, the coordination with many unaffiliated organizations to issue new keys is eliminated. The issuer simply issues a new card with new proxies on the card.

[0069] Such a system as will be readily apparent, can be easily implemented in the system of Figures 1-12 to provide enhanced functionality and flexibility.

[0070] Although the invention has been described with reference to these preferred embodiments and features, other similar embodiments and features can achieve the same results. Variations and modifications of the present invention will be apparent to one skilled in the art and the present disclosure is intended to cover all such modifications and equivalents.

Claims

1. A system for selective organization, access to and use of personal data, comprising:

a server, having data storage means for storing personal data in three separate and distinct data stores;

a first data store stored on said data storage means comprising static identification data which is personal to a user having access means for connecting to the server accessing and using;

a second data store stored on said data storage means comprising moderately dynamic personal data about the user; and

a third data store stored on said data storage means comprising dynamic demographic information data about the user.

2. A system according to claim 1 further comprising access means for connecting to said server to access said first, second and third data stores.

3. A system according to claim 2 wherein said access means comprises a computer terminal connectable to said server via a network.

4. A system according to claim 2 wherein said access means comprises an electronic wallet having said first data store duplicatively stored therein, portions of said second data store and portions of said third data store stored therein.

5. A system according to claim 1 further comprising authorizing means for allowing selected users access to and use of dynamic personal information data in said third data store.

6. A system according to claim 5 further comprising matching means for matching selective dynamic personal information data in said third data store which is specific to a consumer with selected information provided by said selected users.

7. A system according to claim 1 further comprising means for authenticating and signing documents for a user from data obtained from said second data store in communication with a user.

8. A system according to claim 1 further comprising means for matching a user profile obtained from said third data store, with a merchant profile, upon user request, for transmitting information about the merchant's products to the user.

9. A system according to claim 1 wherein said data in said third data store is stored in a configuration ensuring user anonymity.

10. A system according to claim 1 wherein said second data store includes credited value data for use by a user in commercial transaction.

11. A method of selectively organizing, accessing and using personal data comprising:

storing a first data store made up of data comprising static identification data which is personal to a user having access to the first data store;

storing a second data store made up of data comprising moderately dynamic personal data about the user having access to the second data store; and

storing a second data store made up of data comprising dynamic demographic information data about the user having access to the third data store.

12. A method as in claim 1 further comprising providing access by a user to said first data store for using the data therein for filling out forms.

13. A method as in claim 1 further comprising duplicating the data in the first data store, and portions of the data in the second and third data stores, on an electronic wallet.

14. A method as in claim 1 further comprising making data about selected users in the third data store available on an anonymous basis to merchants to allow merchants to provide information to the users about merchant products or services that match the data provided.

15. A method as in claim 1 further comprising downloading purchasing credits from said second data store into an electronic wallet to allow a user to engage in commercial transactions with such credits.

16. A method as in claim 1 further comprising monitoring certain groups of data in said second data store for the occurrence of certain events, and notifying a user corresponding to said data of the event.

17. A method as in claim 16 further comprising accessing outside data sources to update data in said second and third data stores on a periodic basis.

18. A method as in claim 1 further comprising authorization by a user to allow selected third parties to access data in said second data store.

19. A method as in claim 18 wherein said third parties are doctors.

20. A method as in claim 18 wherein said third parties are financial service providers.

21. A method as in claim 18 wherein said third parties

are one of the group consisting of telephone service vendors, power service vendors, and cable television vendors, insurance vendors, and credit card providers.

5

10

15

20

25

30

35

40

45

50

55

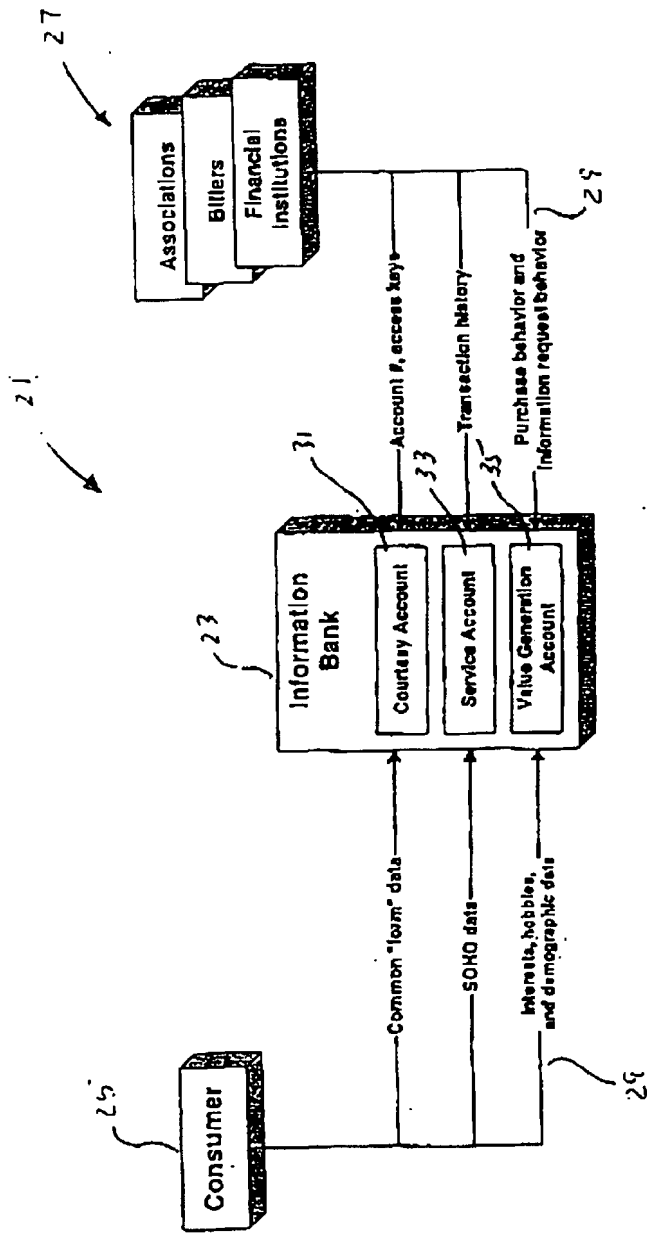


FIG. 1

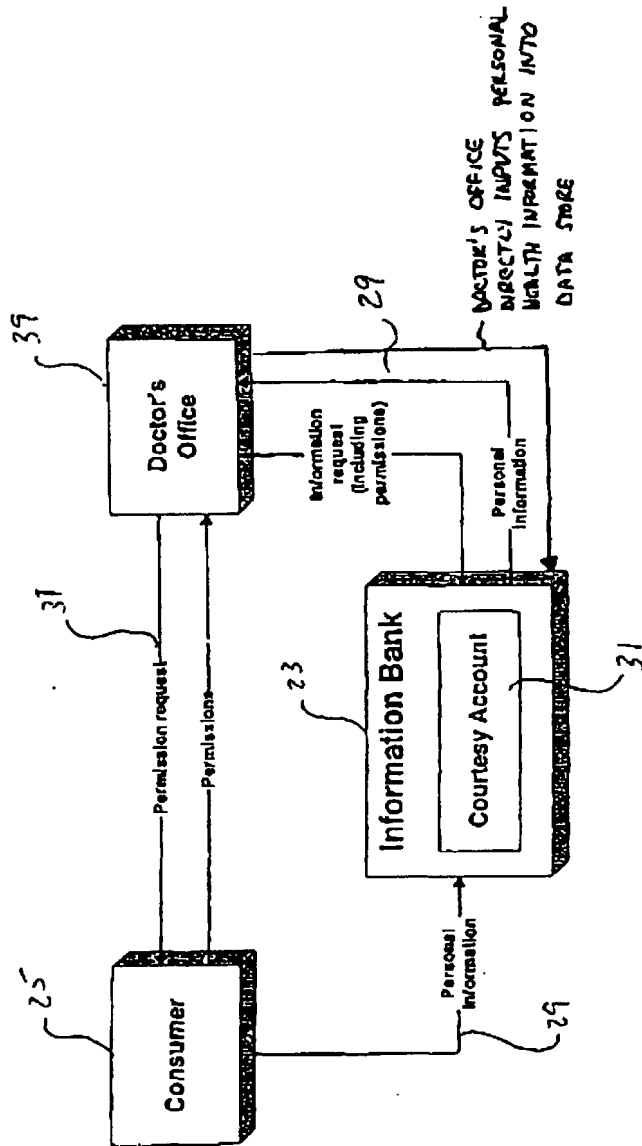


FIG. 2

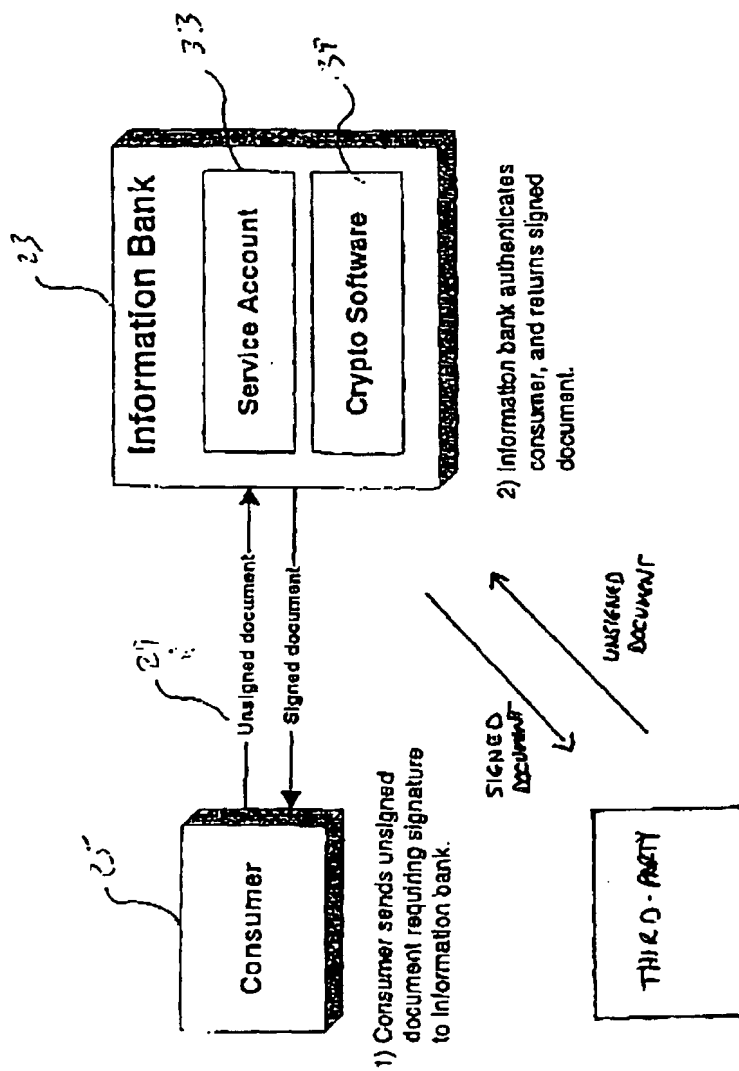


FIG. 3

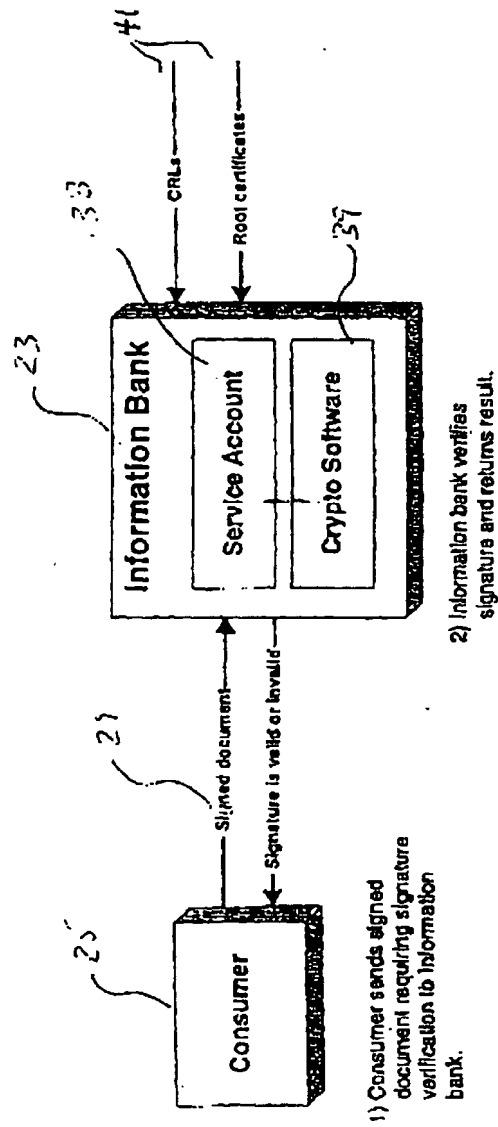


FIG. 4

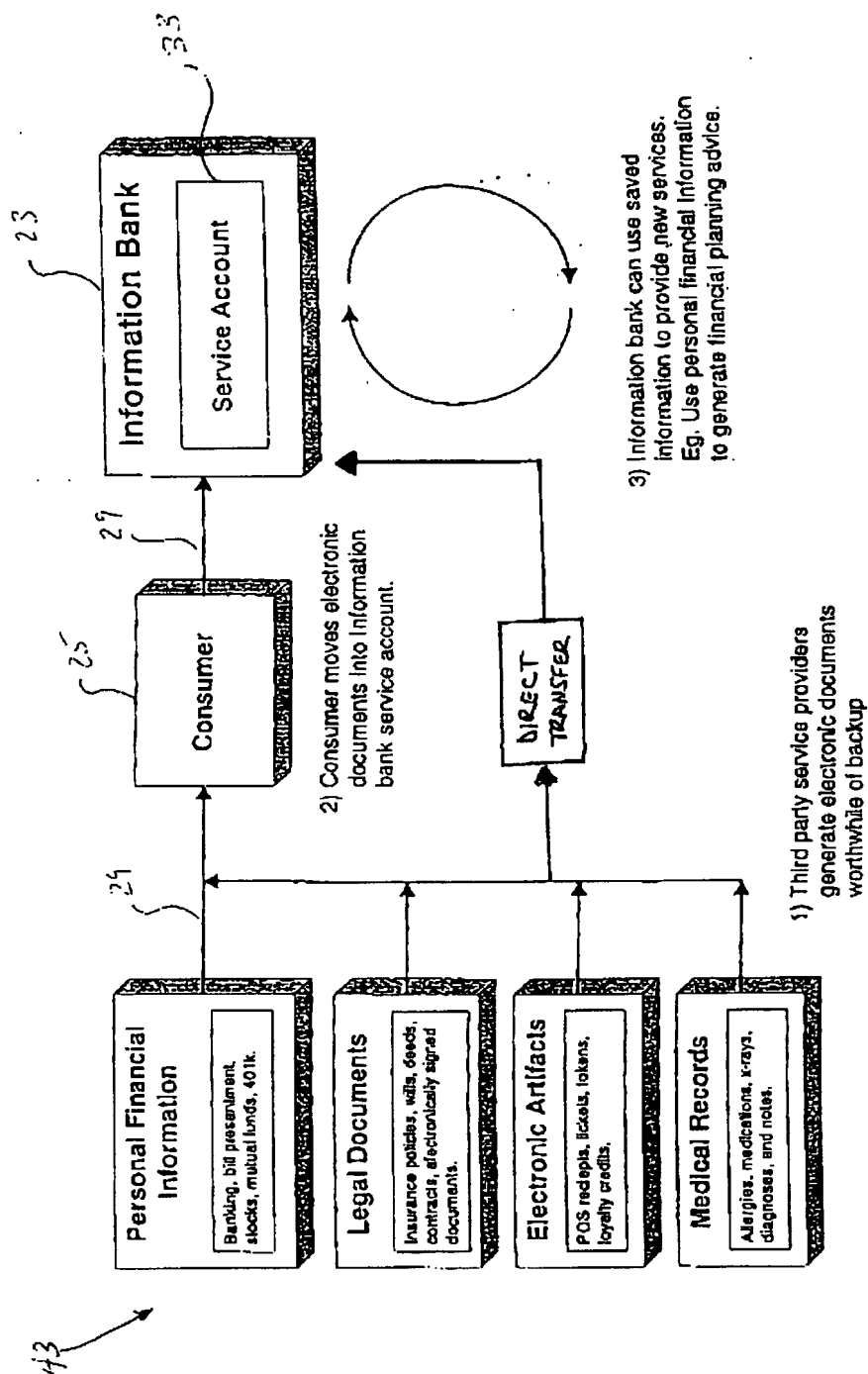


FIG. 5

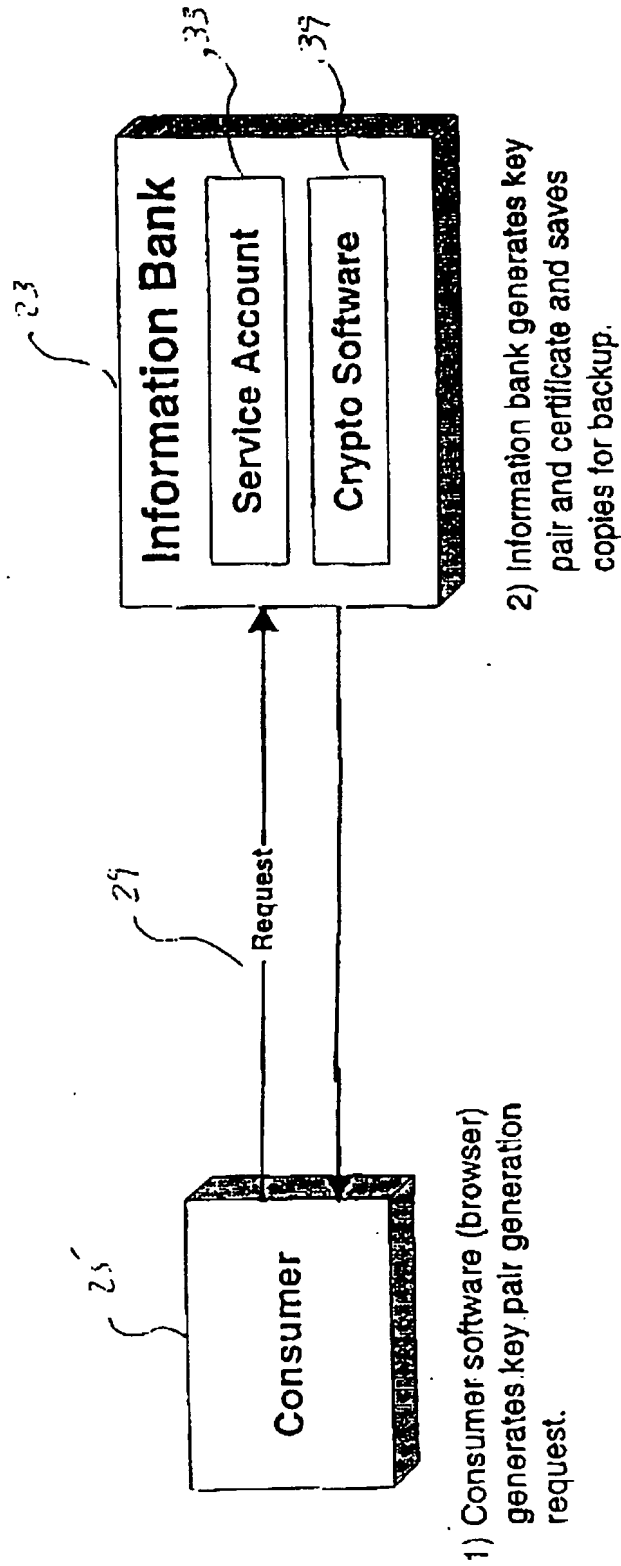


FIG. 6

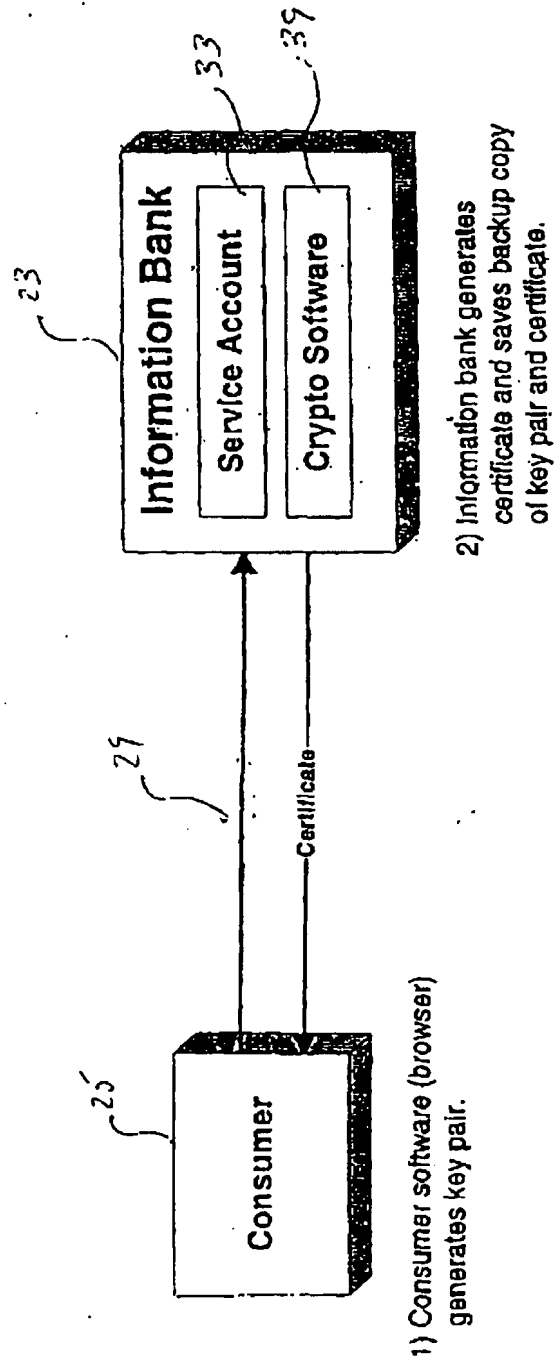


FIG. 7

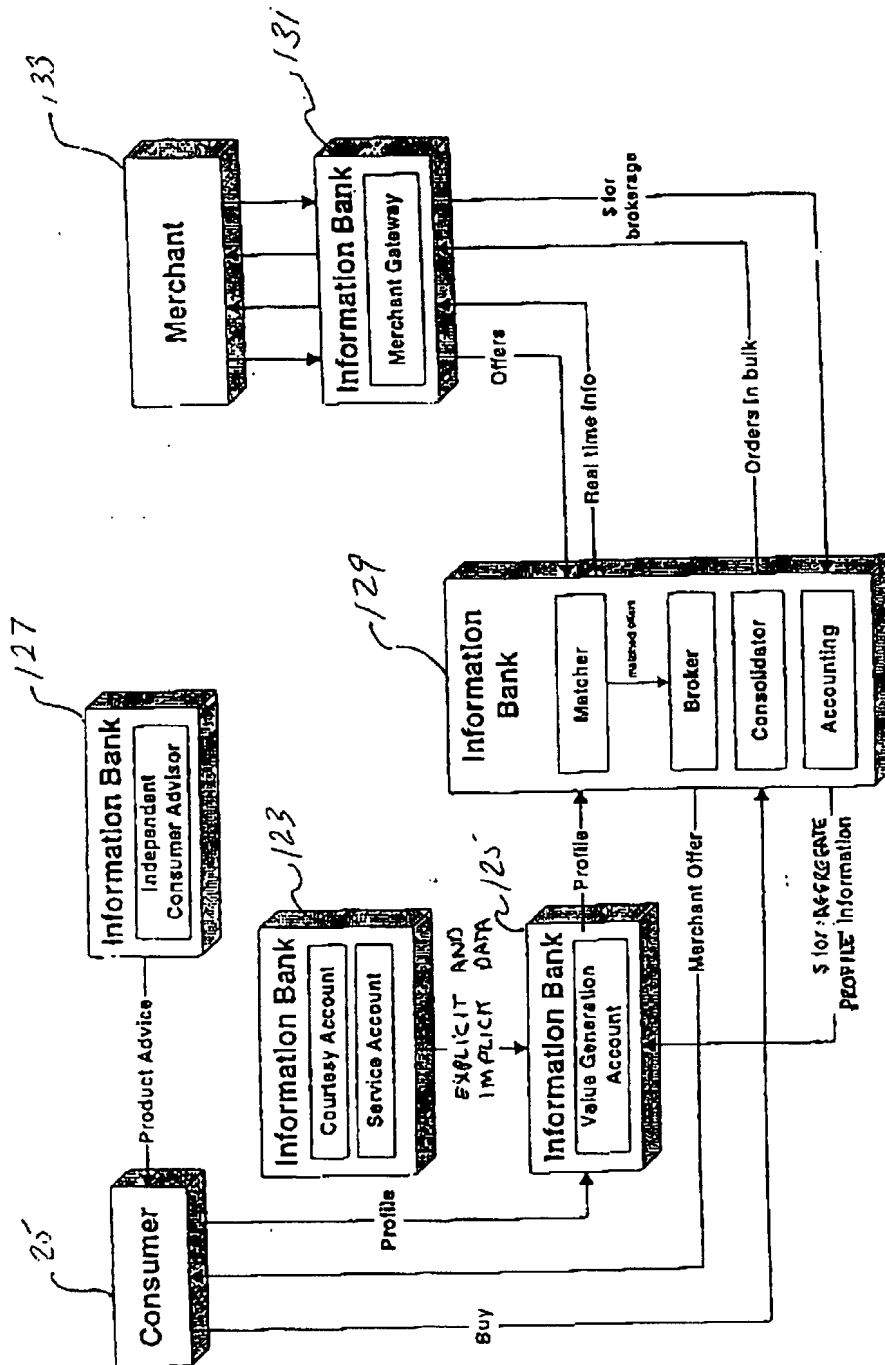


FIG. 8

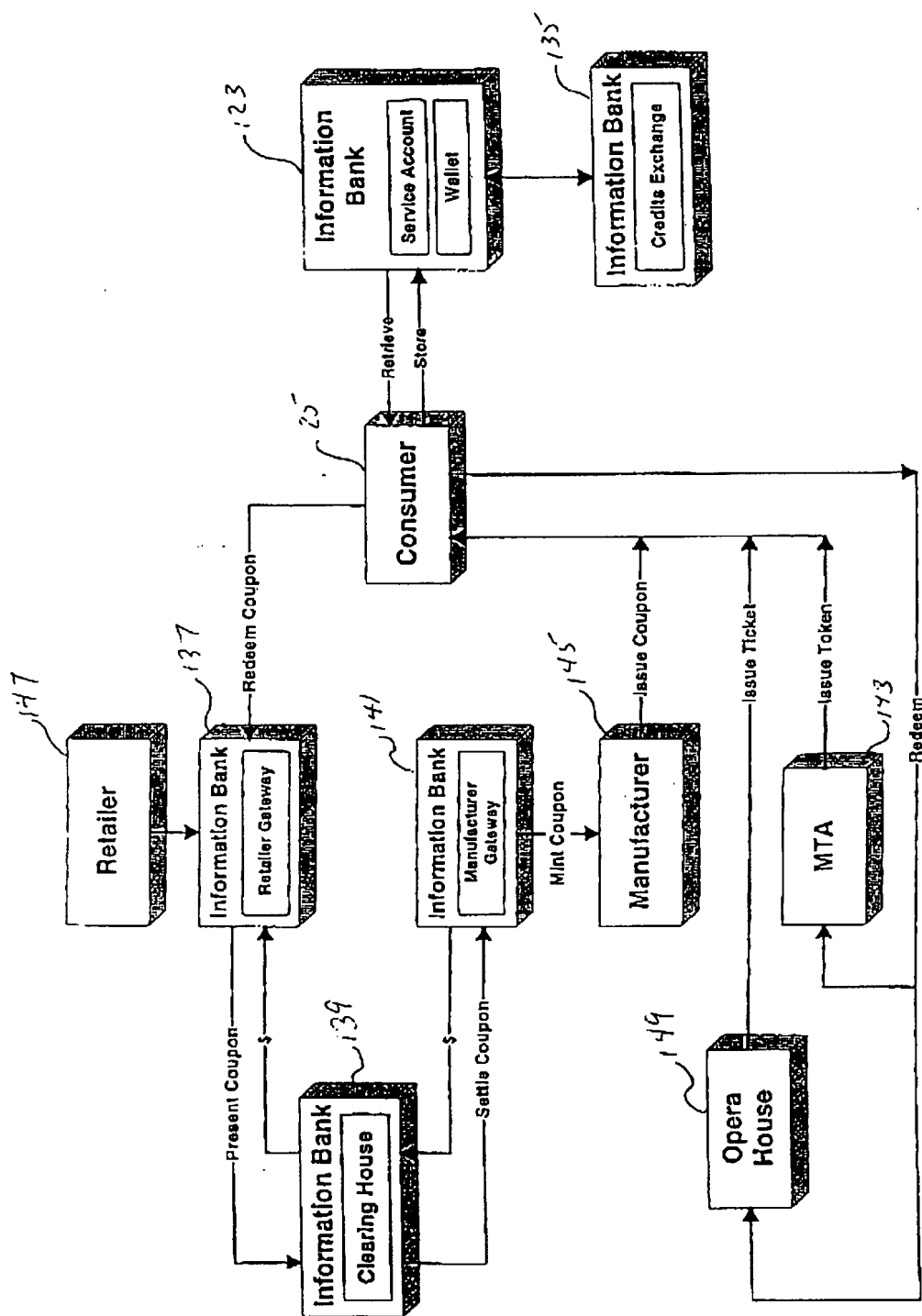


FIG. 9

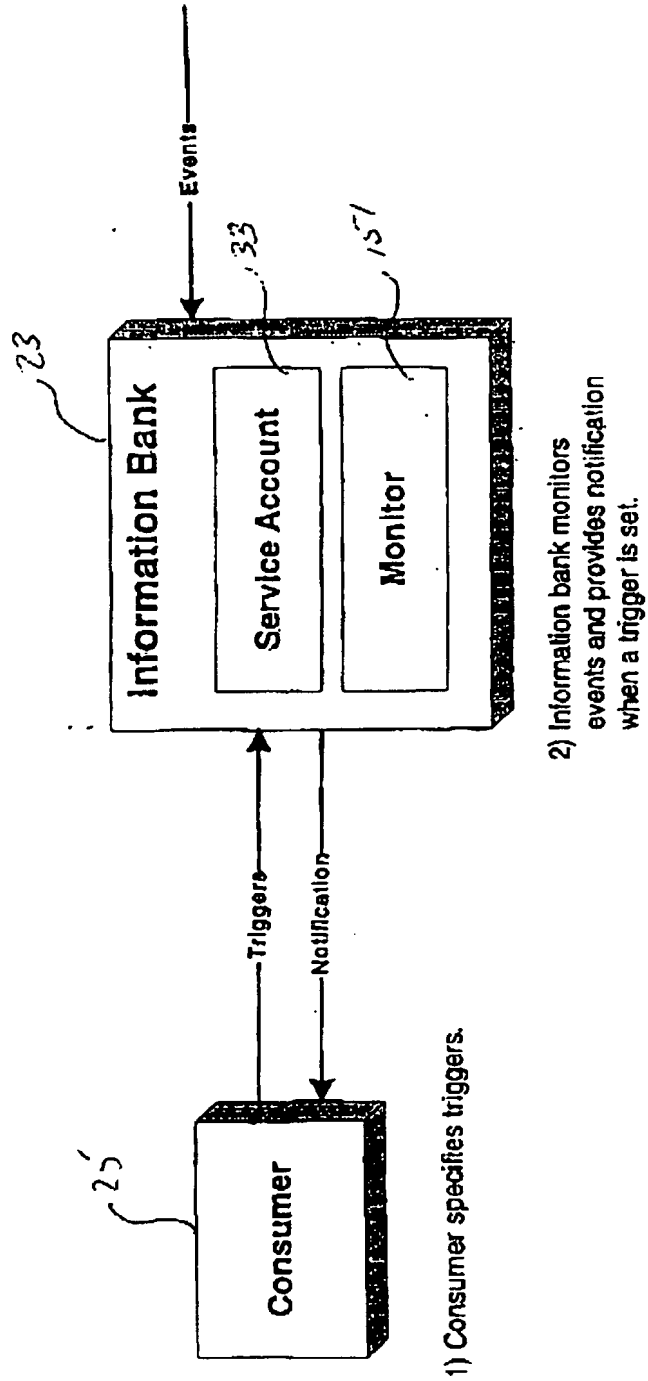
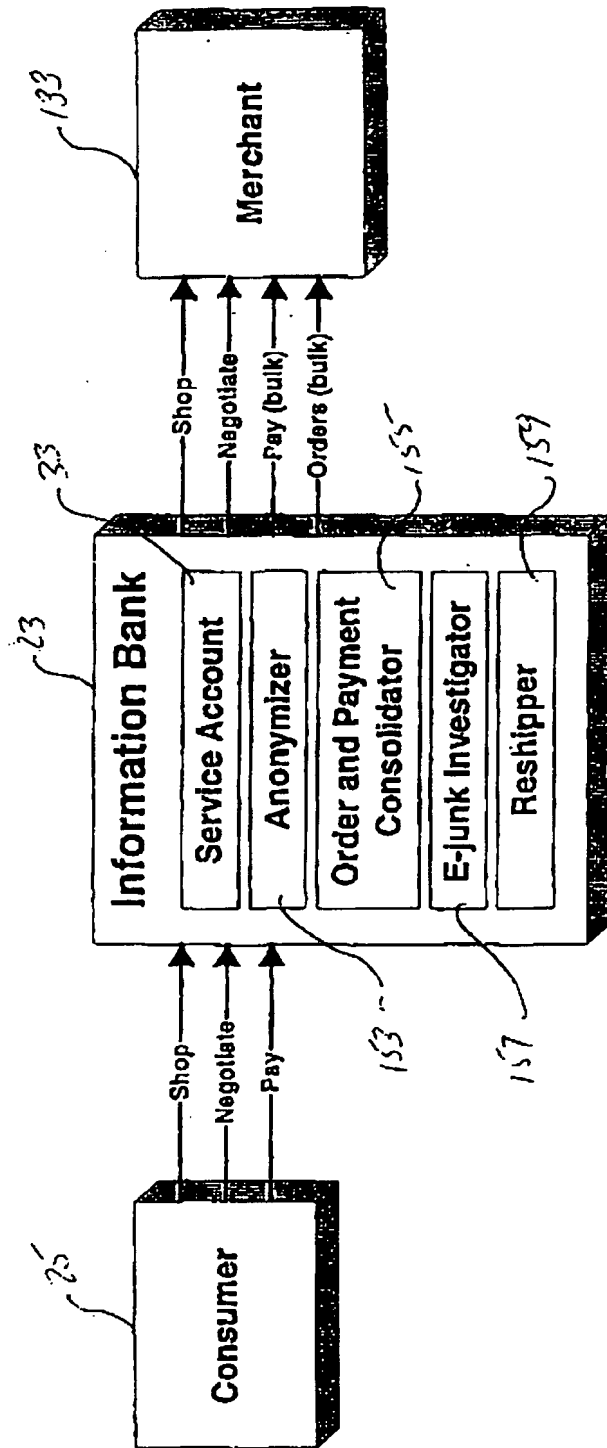


FIG. 10



1) Information bank intermediates consumer interaction with merchant in order to anonymize.

FIG. 11

Information Banking		
Courtesy Account	Service Account	Interest Bearing Account
<p>Definition: A free account that consumers get as a courtesy for being a customer. Certain services that come with it are also gratis.</p>	<p>Definition: A consumer payed for account. They pay for long term, guaranteed safe storage; and external access by authorized people (Dr's, Account's, etc)</p>	<p>Definition: In return for making certain personal types of information available, the consumer is payed a portion of the receipts of selling that data. No names nor address are ever revealed.</p>
<p>Characterized by: Small amount of data Relatively static Indefinite storage time</p>	<p>Characterized by: Large amount of data Dynamic Stored over long periods of time</p>	<p>Characterized by: Demographic data Users interests User profiles User agents</p>
<p>Examples: Name, Address, Phone, Social Security #, and other commonly asked for information on forms, applications, etc.</p>	<p>Examples: Billing history, payment history, loans, real estate holdings, stock, bond, fund holdings, medical records, home web pages, etc</p>	<p>Examples: Age, geographic location, race, religion, professional interests, hobby interests, frequent purchase categories, explicit requests for information, explicit requests for blocking categories of information</p>
<p>Service Examples: Automated form filling Safe Shopping General E-Commerce</p>	<p>Service Examples: Bill presentment / Payment Relationship management Anywhere, Anytime access Guaranteed data safe Tax preparation Emergency information focal point</p>	<p>Service Examples: Solicited Agent searches Pay to contact unsolicited offers Market Research Electronic Census Profile oriented special offers</p>
Free to Consumer	Consumer pays	Consumer gets \$\$

FIG. 12

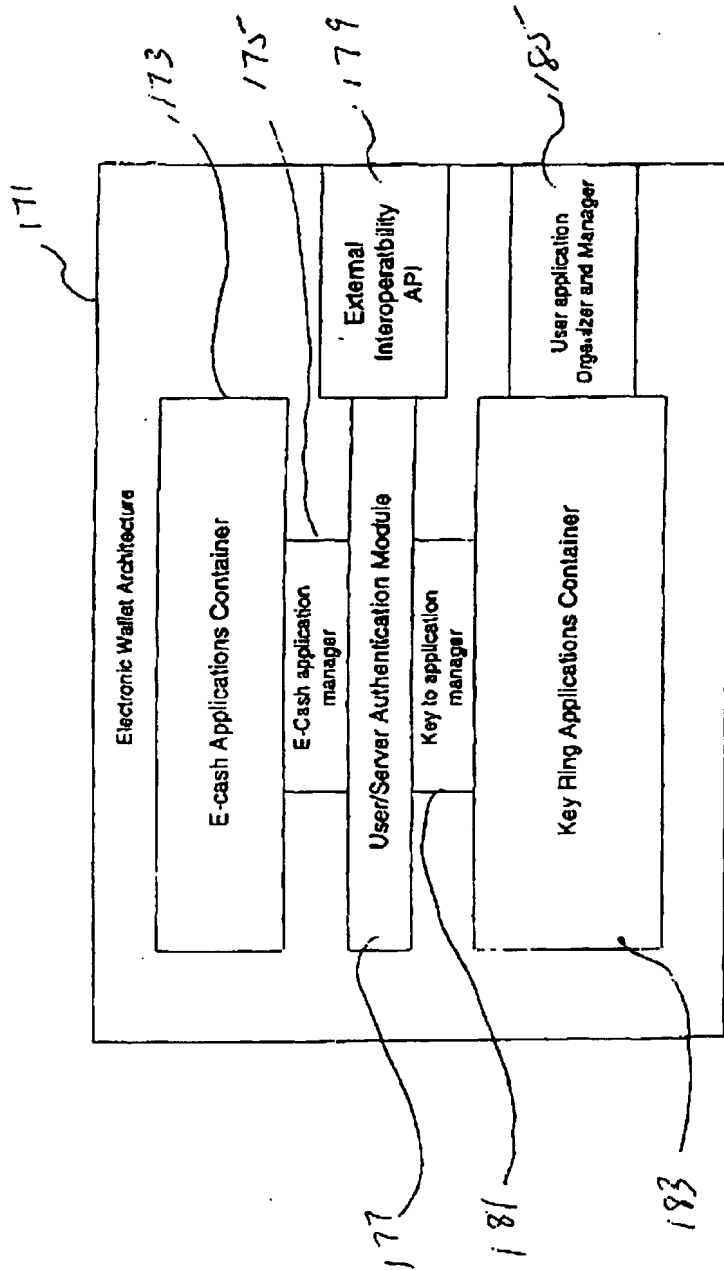


FIG. 13

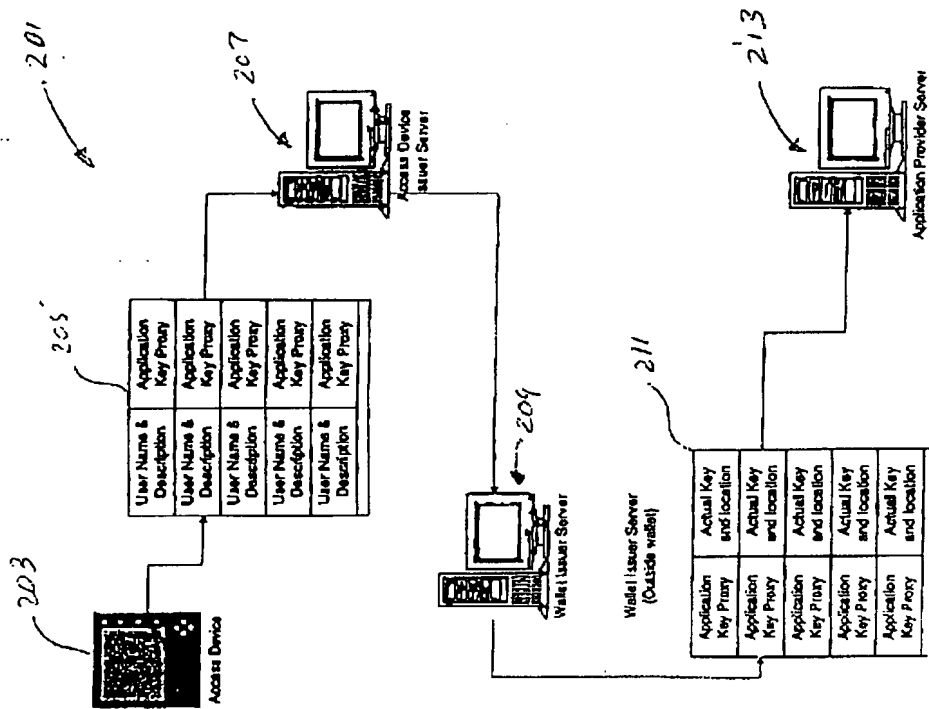


FIG. 14